OcNOS®

Open Compute
Network Operating System
for Service Providers
Version 4.0

OcNOS Configuration Guide

January 2021

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

Preface

This guide describes how to configure OcNOS.

Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Related Documentation

For information about installing of OcNOS, see the *Installation Guide* for your platform.

Feature Availability

The features described in this document that are available depend upon the OcNOS SKU that you purchased. See the *Application Notes* for a description of the OcNOS SKUs.

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

SP 3.0 New Features

Control Plane policing (CoPP):

- Chapter 1, *Control Plane Policing Configuration*
- Chapter 1, *Control Plane Policing Commands*

ISIS IPv6:

- Chapter 7, *IS-IS IPv6 Configuration*
- Chapter 5, *ISIS IPv6 VRF Configuration*

Optical Line Termination (OLT):

- Optical Line Termination Configuration Guide
- Optical Line Termination Command Reference

Layer 2 subinterface:

- Chapter 14, *Layer 2 Subinterface Configuration*
- Chapter 9, *Layer 2 Subinterface Commands*

Layer 3 subinterface:

- Chapter 15, *Layer 3 Subinterface Configuration*
- Chapter 1, *Layer 3 Subinterface Commands*

Precision Time Protocol (PTP) G.8275.1 (T-GM) with GPS:

- Chapter 1, *Boundary Clock Configuration*
- Chapter 1, *PTP 8275.1 and PTP 8275.2 Commands*

Synchronous Ethernet:

- Chapter 1, *SyncE Commands*
- Chapter 2, *SyncE Show Commands*

Layer 2 Multicast Listener Discovery (MLD) Snooping:

- Chapter 4, *Layer 2 MLD Snooping Commands*

6PE Inter-AS option-B:

- BGP Labeled Unicast with Inter-AS

MPLS VPN Inter-AS Option-B:

- neighbor allow-ebgp-vpn

MPLS ping and trace route:

- ping
- traceroute

DHCP relay with option 82:

- DHCP Relay option 82
- ip dhcp relay information option
- ip dhcp relay information source-ip

ACL over Loopback

Passwordless SSH

- SSH Key-Based Authentication

SP 1.0 ED 2.4 New Features

Chapter 1, *Control Plane Policing Configuration*

Chapter 5, *VXLAN Tunnel Over SVI*

ACL over Virtual Terminal

EVPN VxLAN:

- Chapter 2, *VXLAN Quality of Service Commands*
- Chapter 3, *VxLAN Multi-Homing Configuration*

CFM Performance Monitoring for VPWS:

- Chapter 4, *Y.1731 Performance Monitoring Configurations*
- Chapter 3, *CFM and Y.1731 Commands*

Ethernet Ring Protection Switching (ERPS):

- Chapter 5, *G.8032 ERPS Version 2*
- Chapter 4, *G.8032 ERPS Version 2 Commands*

Two-way Active Measurement Protocol (TWAMP):

- Chapter 16, *Two-way Active Measurement Protocol*
- Chapter 1, *TWAMP Commands*

IP Fast Reroute/Loop Free Alternate for ISIS/OSPF:

- Loop-Free Alternate Fast Reroute (OSPFv2)
- Loop-Free Alternate (LFA) ECMP PATH (OSPFv2)
- IS-IS IPv4 Loop-Free Alternate Fast Reroute
- LFA Tie-Breaker (ISISv4)
- LFA Termination (ISISv4)
- LFA For ECMP Paths (ISISv4)

Chapter 18, *VLAN Service Queuing (VLAN Shaping)*

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority            Application Priority
  arp                             Internet Protocol (IP)
  bfd                             Bidirectional Forwarding Detection (BFD)
  bgp                             Border Gateway Protocol (BGP)
  bi-lsp                          Bi-directional lsp status and configuration
  bridge                          Bridge group commands
  ce-vlan                         COS Preservation for Customer Edge VLAN
  class-map                       Class map entry
  cli                             Show CLI tree of current mode
  clns                            Connectionless-Mode Network Service (CLNS)
  control-adjacency               Control Adjacency status and configuration
  control-channel                 Control Channel status and configuration
  cspf                            CSPF Information
  customer                        Display Customer spanning-tree
  cvlan                           Display CVLAN information
  debugging                       Debugging functions (see also 'undebug')
  etherchannel                    LACP etherchannel
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip         ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type n to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh in xe0
```

is an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                         ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table P-2 describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
UPPERCASE	See Variable Placeholders	IFNAME
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`

Table P-2: Syntax conventions (Continued)

Convention	Description	Example
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table P-3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

Table P-4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

Table P-5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor

Table P-5: Keyboard operations (Continued)

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
...skipping
interface xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[3-4]

...skipping
```

```
interface xe3
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The `last` modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-6 lists the command modes common to all protocols.

Table P-6: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, `list`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family.

Table P-6: Common command modes (Continued)

Name	Description
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

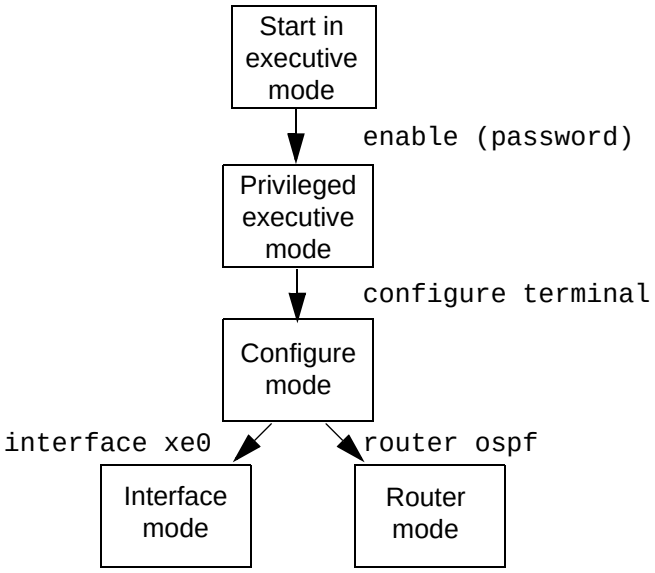


Figure P-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

SECTION 1 Architecture

Architecture Guide

Contents

This document contains this chapter:

CHAPTER 1 Architecture Overview

This chapter introduces OcNOS and describes its high-level architecture.

OcNOS is an industry-standard network operating system with advanced networking features to meet the demands of data center, enterprise, and service provider networks.

The OcNOS networking protocol modules conform to leading IEEE, IETF, and other industry-specific standards:

- Layer 2 switching: VLANs, Spanning Tree
- Layer 3 routing: OSPFv2, OSPFv3, BGPv4, IS-IS
- MPLS: LDP, RSVP, L2VPN, L3VPN
- Carrier Ethernet
- Data center Ethernet

OcNOS provides configuration management through these layers:

- Command line interface
- SNMP

High-Level Architecture

Figure 1-1 shows the high-level architecture of OcNOS.

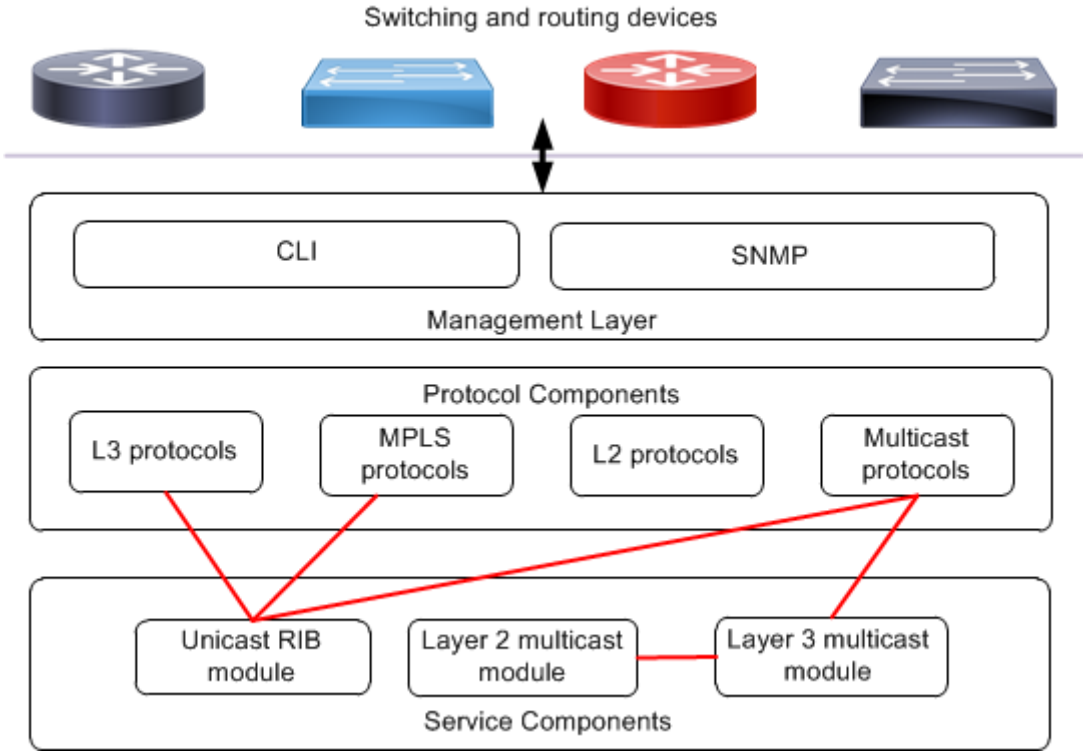


Figure 1-1: OcNOS high-level architecture

The major components of OcNOS are grouped into these categories:

- The Management Interface that is used to configure and operate the OcNOS routing and switching protocols.
- Protocol components, which include:
  - Layer 2 Protocols
  - Layer 3 Protocols
  - Multi Protocol Label Switching Protocols
  - Multicast Protocols
- Service components, which include:
  - Unicast Routing Information Base Module
  - Layer 2 Multicast Module
  - Layer 3 Multicast Module

Management Interface

OcNOS provides a comprehensive set of tools to manage, configure, and operate the routing and switching protocols.

The management interface includes:

- Command Line Interface
- Simple Network Management Protocol

Command Line Interface

The OcNOS command line interface (CLI) offers complete, unified management of OcNOS. Each command is usually associated with a specific task.

The IMI (Integrated Management Interface) shell is a interactive program for managing the OcNOS configuration. The IMI shell connects locally from the console of a device running OcNOS or remotely from a terminal emulator program such as `ssh` or `telnet`.

Through the IMI shell, a system administrator can configure and monitor all of the OcNOS protocols through one centralized connection. The IMI shell stores configuration data and offers extensive monitoring and logging capabilities.

The CLI can use the secure authentication methods of the operating system to manage and validate user names and passwords.

Note: The Linux `bash` shell can also be used to apply non-networking commands directly to the Linux system. However network-related commands such as `ifconfig`, `route`, `vconfig`, `iptunnel`, `brctl`, `ipmaddr`, or their iproute2 equivalents are not supported. The equivalent settings must be configured via the IMI shell in OcNOS.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework has three parts:

- SNMP manager: A system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports data to SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables on the managed device which network management agents can extract from the OcNOS protocols for all standard defined MIBs.

OcNOS supports the AgentX (Agent Extensibility) protocol defined by RFC 2741 to communicate between the subagent and the master agent. As shown in Figure 1-2, an SNMP manager on the network sends query packets to gather status data. Each OcNOS protocol responds to these queries as defined by the corresponding MIB for the protocol.

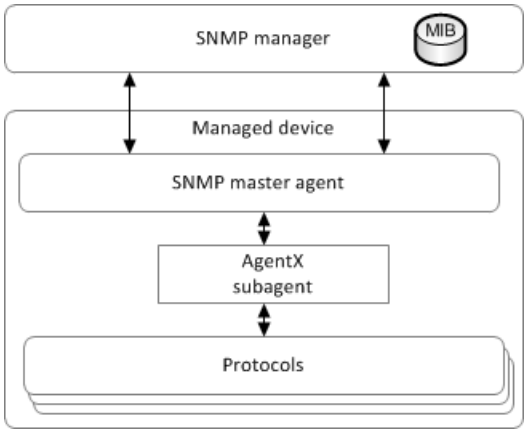


Figure 1-2: SNMP subagent

OcNOS can log both system events and errors.

For details about the MIBs that OcNOS supports, see the MIB compliance documents.

Layer 2 Protocols

OcNOS includes these Layer 2 features:

- Virtual Local Area Networks
- Spanning Tree
- Carrier Ethernet
- Link Aggregation (802.1AX)
- Multi-Chassis Link Aggregation

Virtual Local Area Networks

The VLAN modules offer consistent network-wide management tools to manage virtual LANs (Local Area Networks) and bridged VLANs:

- VLAN bridging divides a single physical LAN into two or more VLANs. Each VLAN is a collection of some of the LAN nodes grouped together to form individual broadcast domains.
- VLANs, in accordance with IEEE 802.1Q, enable multiple bridged LANs to transparently share the same physical network link without leaking information between LANs. Traffic between VLANs is restricted to bridges that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

OcNOS VLAN modules make it easy to administer logical groups of stations that can communicate as if they were on the same LAN. They make it easier to manage a move, add, delete, or other updates to members of these groups.

The following highlights the features of the VLAN modules.

MAC Bridging (802.1d)

The OcNOS VLAN modules support all IEEE 802.1D LAN MAC (Media Access Control) protocols, shared media, and point-to-point LANs. MAC bridging allows multiple LANs to be connected together. MAC bridging filters data sent between LAN segments, reduces network congestion, and allows networks to be partitioned for administrative purposes.

Provider Bridging (802.1ad)

Provider Bridging (PB) enables a service provider to use the architecture and protocols of 802.1Q to offer the equivalent of separate Local Area Networks (LANs), bridged LANs, or virtual bridged LANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customers and the service provider.

When VLANs were originally defined in the 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, thus this limit could prevent a provider from having more than 4096 subscribers.

To overcome the 4096 VLAN identifier limit, the frame format for 802.1ad inserts an additional VLAN header into a single 802.1Q Ethernet frame. There are two types of VLAN headers:

- The C-VLAN or inner header which is closest to the payload portion of the frame identifies the customer VLAN
- The S-VLAN or outer header which is closest to the Ethernet header identifier the provider VLAN

The frame format for 802.1ad is also called “Q-in-Q” or “double tagged”.

With the two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 labels.

VLAN Prioritization (802.1p/Q)

OcNOS includes priority signaling for traffic at the data-link layer. IEEE 802.1Q specifies a priority value of between 0 and 7 inclusive that can be used by QoS (Quality of Service) disciplines to differentiate traffic. Although this technique is often called “802.1p”, there is no standard by that name published by the IEEE. Instead, the technique is now incorporated into 802.1Q standard.

Spanning Tree

The OcNOS Spanning Tree support are a combination of these modules:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

The following highlights the features of the Spanning Tree Protocol modules.

Note: All OcNOS spanning tree modules support 802.3x flow control, broadcast storm recovery, and port mirroring.

Spanning Tree Protocol (802.1d)

The OcNOS Spanning Tree Protocol (STP) module creates spanning trees within mesh networks of Layer 2 connected bridges, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes.

STP devices exchange BPDU (bridge protocol data unit) messages. The Spanning Tree Algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network architects can design a topology that uses redundant links as automatic backup paths in the case of active link failure. Automatic backup takes place without the pitfalls of bridge loops, or the need to manually enable or disable backup links.

Rapid Spanning Tree Protocol (802.1w)

The Rapid Spanning Tree Protocol (RSTP) accelerates the re-configuration and restoration of a spanning tree after a link failure.

Multiple Spanning Tree Protocol (802.1s)

The Multiple Spanning Tree Protocol (MSTP) is a supplement to the IEEE 802.1ad standard. MSTP allows VLAN bridges to use multiple spanning trees, by providing the ability for traffic belonging to different VLANs to flow over potentially different paths within the virtual bridged LAN.

Carrier Ethernet

OcNOS offers a comprehensive set of Carrier Ethernet (CE) protocols from the IETF and IEEE.

Provider network operators can also benefit from Provider Bridging (802.1ad).

Link Level Discovery Protocol (802.1AB)

Link Layer Discovery Protocol (LLDP) is an agent running on an IEEE 802.1 bridge that provides a mechanism for all the bridges connected to the LAN to send and receive connectivity and management related information to each other.

Link Aggregation (802.1AX)

The link aggregation module allows one or more links to be aggregated together to form a Link Aggregation Group (LAG), such that a MAC client can treat the Link Aggregation Group as if it were a single link. The Link Aggregation Control Protocol (LACP) allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The system treats the aggregated interface as a single interface. When there is a failure in one physical interface, the remaining interfaces stay up, so there is no data traffic disruption. Link aggregation is defined in IEEE 802.1AX.

Multi-Chassis Link Aggregation

In data centers, spanning tree protocols like STP, RSTP, and MSTP create a loop-free topology that results in under-utilized physical links as well as redundant links between nodes that are in discarding state. As a result, more than 50% of the physical links are blocking. Link Aggregation (802.1AX) binds multiple physical links in a node into a single logical link, thereby increasing bandwidth and providing link-level redundancy. As a result, physical link utilization improves. However, a node failure in the network causes complete traffic loss as link aggregation does not provide any node-level redundancy.

The OcNOS implementation of multi-chassis link aggregation (MC-LAG) extends the link aggregation concept to ensure that connectivity between two networks can be maintained despite the failure of a node. MC-LAG provides node-level redundancy by allowing two or more nodes in the network to share a common LAG endpoint. MC-LAG emulates multiple nodes to represent a single logical node to the remote node running link aggregation. Even if one of the nodes is down, there exists a path to reach the destination via other nodes. MC-LAG allows you to use all interconnects in an active/active mode.

As shown in Figure 1-3, switch 2 and switch 3 share a common endpoint in switch 1. Switches 2 and 3 are a single logical node to switch 1. Even if switch 2 or switch 3 is down, there exists a path from switch 1 to reach other destinations. Switch 2 and switch 3 also share a common endpoint in switch 4.

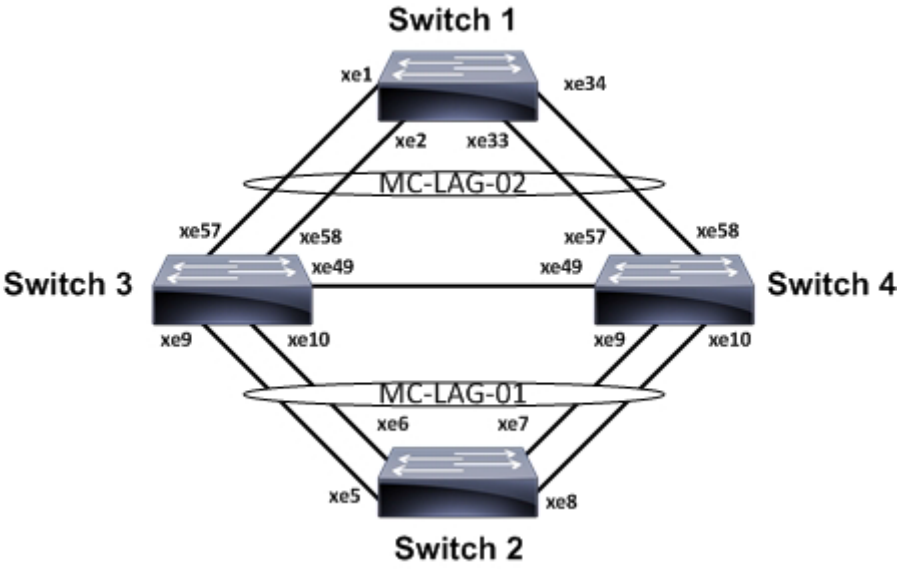


Figure 1-3: MC-LAG switching topology

With MC-LAG, at either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. In Figure 1-3, switches 1, 2, and 3 are a portal system, each with physical links that together make up a link aggregation group. The portal's systems cooperate to emulate the presence of a single aggregation system to which the entire link aggregation group is attached. Switches 2, 3, and 4 are also a portal system.

MC-LAG is also called MLAG.

Layer 3 Protocols

OcNOS supports these IP protocols:

- Border Gateway Protocol
- Open Shortest Path First
- Intermediate System to Intermediate System
- Virtual Router Redundancy Protocol
- Bidirectional Forwarding Detection

In addition to the standard Layer 3 routing protocols, OcNOS offers:

- Virtual Routing and Forwarding (VRF) support
- Constrained Shortest Path First (CSPF) topology support for the Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) protocols

Unicast Routing Information Base Module

OcNOS maintains a central unicast Routing Information Base (RIB). A RIB is a data structure stored in a network device that lists the routes to particular network destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as BGP and OSPF. Static fixed routes are added to a RIB by commands. (A RIB is also called a routing table.)

A Forwarding Information Base (FIB) is used to find the proper interface to which an input interface should forward a packet. In contrast to RIBs, FIBs are optimized for fast lookup of destination addresses. (A FIB is also called a forwarding table.)

Protocol modules create their own routes and communicate this protocol-specific information to the unicast RIB. The OcNOS unicast RIB contains all routing information received from routing peers, for example, destination prefix, nexthop information, and distance.

Figure 1-4 shows how the Layer 3 protocols and the unicast RIB communicate.

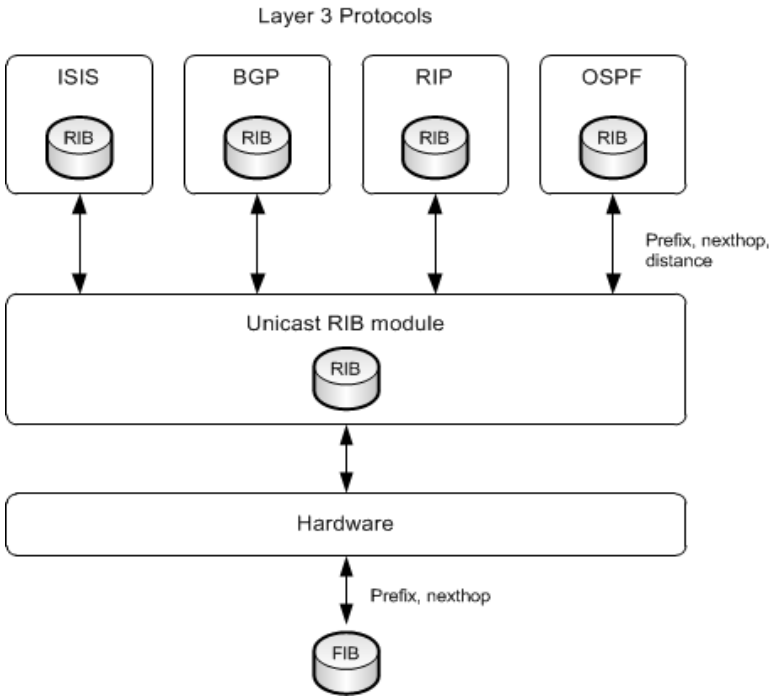


Figure 1-4: Protocol, unicast RIB, and kernel interaction

The unicast RIB performs these operations:

- Communicate with OcNOS routing and switching modules to get routing information updates
- Provide configuration for static routes
- Process the routing information and maintain all the received routes from clients as part of the RIB
- Maintain the FIB
- Process the routes and select the FIB route and program the kernel
- Redistribute routes
- Handle interface up and down events

For every known prefix, OcNOS maintains a route node entry in its RIB. OcNOS populates this table upon receiving routes from:

- Protocols such as BGP and OSPF
- Static routes configured using commands
- The kernel FIB
- Connected routes derived from interface information

Routing protocols use different metrics to calculate the best path for a destination.The best path is sent to the RIB.

Border Gateway Protocol

Border Gateway Protocol (BGP) is a core exterior gateway protocol (EGP) used on the Internet. BGP maintains a table of IP networks, or prefixes, which designate network reachability among Autonomous Systems (AS). BGP is a path-vector protocol that makes routing decisions based on path, network policies, and/or rule sets.

OcNOS supports BGP version 4 and offers VPN extensions for MPLS-VPN support. The VPN extensions work with MPLS-LDP and RSVP.

OcNOS BGP features include:

- IPv4 support
- Route Reflection
- Route Refresh
- Community Attributes
- Community Attributes in Multi-Home Routing
- Extended Communities
- Protection of BGP Session via the TCP MD5 Signature Option
- Capabilities Advertisement
- Route Flap Damping
- E-BGP Multi hop
- Stateful implementation
- Multi-protocol BGP (MP-BGP) extensions
- BGP/MPLS VPNs
- Graceful restart
- BGP Inter-Domain Routing (IDR):
    - Virtual Routing and Forwarding Support
    - Full MIB support

Open Shortest Path First

Open Shortest Path First (OSPF) is a link-state routing protocol that runs internally on a single autonomous IPv4 system. Each router designated to run OSPF maintains an identical database only within area. From this database, a routing table is calculated by constructing a shortest-path tree.

OcNOS OSPF features include:

- Opaque Link State Attributes (LSA)
- Link State Attributes (LSA) - Throttling
- Link Local Signaling
- Multiple Instance Support
- Intra- and inter-area routing
- Type 1/2 external routing
- Opaque link state availability (LSA) Option
- Manual and automatic virtual links
- Broadcast, point-to-point and point-to-multi-point models, NBMA network

- MD5 authentication
- Incremental SPF
- Traffic Engineering extensions
- Virtual Routing (VR) and Virtual Routing and Forwarding (VRF) support
- Graceful restart
- Virtual Private Network (VPN) support
- Constrained Shortest Path (CSPF) support
- Full MIB support

Intermediate System to Intermediate System

Intermediate System-to-Intermediate-System (IS-IS) is a link-state routing protocol that runs internally on a single autonomous system. IS-IS routers maintain identical databases that describe the autonomous system's topology. A routing table is calculated from the database by constructing a shortest-path tree.

OcNOS IS-IS features includes:

- Use of OSI IS-IS for Routing in TCP/IP
- Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- IS-IS Exponential Back-off of SPF
- IS-IS external routes redistribution
- BFD over IS-IS (v4)
- Full MIB support

Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) allows a virtual router composed of two or more routers on the same subnet to prevent failure by providing at least one standby virtual router if the master virtual router fails. VRRP eliminates the single point of failure most common in a static default routed environment.

In OcNOS, the VRRP module functions are to:

- Bring up or down VRRP sessions in the respective VR mode
- Create and delete VRRP sessions dynamically
- Transmit and receive VRRP packets to and from the virtual-router peers based on the time-out value or the current state of the VRRP router

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process manages dynamic fail-over in the forwarding responsibility should the master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first-hop router by end-hosts. The advantage of using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

OcNOS supports VRRP as specified in RFC 5798.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) reduces the reliance upon the relatively slow Hello mechanism in routing protocols to detect failures where no hardware signaling is available to assist. BFD works with BGP, OSPFv2, and IS-

IS to enable them to configure BFD sessions, and for the sessions to receive the bidirectional forwarding failure notifications.

BFD provides the following features:

- A single mechanism to detect liveliness over any media and in any protocol layer
- Rapid detection of communication failures between adjacent systems to quickly establish alternative paths
- Passive, Active, Synchronous, Asynchronous, and Demand modes of operation
- Improved system performance when faster detection is required, because data-plane reachability detection is detached from control-plane functionality
- OcNOS protocol modules support BFD irrespective of where BFD packet-sending operations take place: in the interfaces, data links, or to some extent, in the forwarding engines themselves
- BFD is Graceful-Restart unaware: whenever BFD timers expire, a session-down event is triggered to the protocol module, and BFD maintains sessions for the protocol while it undergoes Graceful Restart
- A fast mechanism to detect liveliness of static next-hops

Multicast Protocols

OcNOS provides these multicast protocols:

- Layer 2 Multicast Module
- Layer 3 Multicast Module
- Protocol-Independent Multicast Module

Layer 2 Multicast Module

Multicast packets are transmitted to a specific multicast address that represents a group of receivers that want to receive the packets. Through the Internet Group Management Protocol (IGMP), a host receiver can join and leave a multicast group.

IGMP snooping is the ability to passively listen for IGMP packets to learn IPv4 multicast group membership information. With IGMP snooping, multicast traffic for a group is only forwarded to ports that have members in that group. OcNOS supports IGMP snooping functionality for IGMP versions 1, 2, and 3.

Layer 3 Multicast Module

The multicast protocols communicate with the Layer 3 multicast module which communicates with the multicast forwarder. A common multicast routing information base allows multiple multicast protocols to function simultaneously.

Figure 1-5 shows the Layer 3 multicast architecture of OcNOS. The Layer 3 multicast module holds the multicast RIB and consolidates the routes from multicast routing protocols such as Protocol-Independent Multicast Module and Multi Protocol Label Switching Protocols and installs them in the multicast FIB.

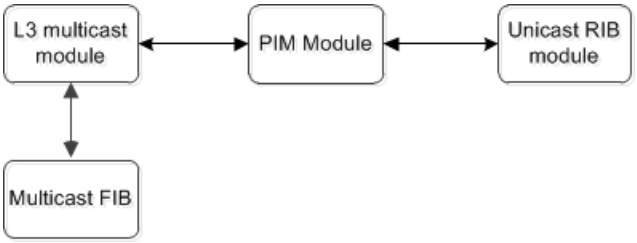


Figure 1-5: Layer 3 multicast architecture

Protocol-Independent Multicast Module

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for IP networks that provides one-to-many and many-to-many distribution of data over a network. PIM is termed *protocol-independent* because it does not have its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.

OcNOS support these variants of PIM:

- PIM Sparse Mode (PIM-SM: RFC 4601) efficiently establishes distribution trees across wide area networks (WANs) by routing packets to multicast groups. PIM-SM constructs a tree from each sender to the receivers in a multicast group and packets from the sender follow the tree to interested recipients. PIM-SM is for situations where multicast groups are thinly populated across a large region. Although it can operate in LAN environments, it is most efficient in WAN environments.
- PIM Source-Specific Multicast (PIM-SSM: RFC 3569) is a subset of PIM-SM that allows deployment of SSM in a network with hosts that do not support IGMP version 3. PIM-SSM builds trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications (mostly broadcasting of content). In PIM-SSM, an IP datagram is transmitted by a source S to an PIM-SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G).

PIM features include:

- Any Cast RP
- Bootstrap router
- PIM border

Multi Protocol Label Switching Protocols

Multi-Protocol Label Switching (MPLS) operates at a layer operated between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer). The MPLS modules support enterprise, edge, and core applications.

The OcNOS MPLS module supports the following protocols and features:

- Resource Reservation Protocol-Traffic Engineering
- Label Distribution Protocol
- Layer 2 Virtual Private Network
- Layer 3 Virtual Private Network

Figure 1-6 shows the MPLS high-level architecture.

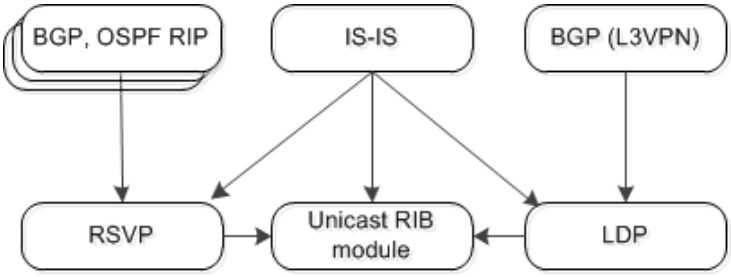


Figure 1-6: MPLS High Level Architecture

Resource Reservation Protocol-Traffic Engineering

Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) communicates with the QoS module to:

- Find if the requested bandwidth is available
- Reserve bandwidth for an LSP
- Release a reserved resource

Label Distribution Protocol

With the Label Distribution Protocol (LDP), two label-switched routers (LSR) exchange label mapping information. The two LSRs are called LDP peers and the exchange of information is bi-directional. LDP is used to build and maintain databases of LSRs that are used to forward traffic through MPLS networks.

LDP works with other routing protocols (such as OSPF and BGP) to create the LSPs used when forwarding packets. An LSP is the path taken by all packets that belong to the Forwarding Equivalence Class (FEC) corresponding to that LSP. In this way, LDP assigns labels to every destination address and destination prefix provided in the OcNOS RIB.

LDP also establishes sessions between non-directly connected peers (targeted LDP).

Layer 2 Virtual Private Network

OcNOS offers MPLS Layer 2 Virtual Private Network (VPN) and Virtual Private LAN Service (VPLS) protocol modules that enhance MPLS by providing transparent LAN access between VPN sites. The VPN infrastructure for the Provider Edge (PE) uses the IP routing, traffic engineering, and MPLS switching features of OcNOS.

Layer 2 VPN connectivity can be implemented by either VPWS (Virtual Private Wire Service) or Virtual Private LAN Service (VPLS):

- VPWS can be only used when interconnecting two sites
- VPLS provides multi-site connectivity and therefore is more flexible

VPLS provides an end-to-end connection over an MPLS tunnel, using a combination of LDP and/or BGP for peer discovery and signaling. Virtual Circuits (VC) create point-to-point VPN connections.

Layer 3 Virtual Private Network

The MPLS Layer 3 VPN is a Provider Edge (PE) technology for service provider VPN solutions. It uses BGP to advertise VPN routes and uses MPLS to forward VPN packets on service provider backbones. A Customer Edge (CE) device first establishes adjacency with a directly connected PE and advertises its VPN routes to the PE and learns remote VPN routes from that PE. A CE and a PE use BGP/IGP to exchange routing information

OcNOS supports BGP-MPLS VPNs for IPv4. Payload data packets are tunneled through the backbone, so that core routers are unaware of IPv4 VPN routes. BGP allocates the labels for these prefixes and then informs its peer about these labels. BGP then installs the labels in the data plane and maps the VPN prefix to the underlying MPLS tunnel. Data traffic is encapsulated with BGP labels and sent on the MPLS tunnel.

System Management

The system management module supports these host protocols:

- Authentication, Authorization, and Accounting
- Dynamic Host Configuration Protocol Client
- Dynamic Host Configuration Protocol Relay
- Domain Name System
- Network Time Protocol
- Remote Authentication Dial In User Service
- Secure Shell
- Simple Network Management Protocol
- Syslog
- Telnet
- User Roles

Authentication, Authorization, and Accounting

The authentication, authorization, and accounting (AAA) commands provide these functions:

- *Authentication* identifies users by asking them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- *Authorization* provides a method of authorizing commands and services on a per user profile basis.
- *Accounting* collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing devices. The AAA feature works with Remote Authentication Dial In User Service.

Dynamic Host Configuration Protocol Client

The Dynamic Host Configuration Protocol (DHCP) client is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

Dynamic Host Configuration Protocol Relay

DHCP relay allows DHCP clients to communicate directly with DHCP servers in small networks with only one IP subnet. To allow DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. The DHCP client broadcasts on the local link and the relay

agent receives the broadcast and transmits it to one or more DHCP servers using unicast. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

Domain Name System

The Domain Name System (DNS) translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

Network Time Protocol

The Network Time Protocol (NTP) synchronizes computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Remote Authentication Dial In User Service

Remote Authentication Dial In User Service (RADIUS) provides centralized Authentication, Authorization, and Accounting management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Secure Shell

Secure Shell (SSH) is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Simple Network Management Protocol

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated and /or encrypted.

SNMP is defined in RFCs 3411-3418.

Syslog

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, applications such as `mail` and `cron` generate messages with facilities named mail and cron.
- Eight degrees of severity (numbered 0-7) of the message.

Telnet

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

User Roles

OcNOS provides four user roles:

- Network Administrator: all access permission to make permanent changes to the switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: all access permission to make permanent changes to the switch configuration. Changes are persistent across reset/reboot of switch. The `start-shell` and `hw-shell` commands are blocked for this role.
- Network Operator: all access permission to make permanent changes to the switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: access permission to display information, but cannot modify any existing configuration.

Virtual Extensible Local Area Network

Virtual extensible LAN (VxLAN) interconnects Layer 2 networks using VxLAN tunnel end points (VTEPs) and a Layer 3 tunnel (segment). A VTEP has an IP address and interacts with a local LAN segment and an IP transport network. A VTEP can be a hypervisor, top-of-rack (TOR) switch, or a gateway. VxLAN can run between VTEPs within a data center or can interconnect different data centers. VxLAN labels Layer 2 segments with a network identifier (VNID) which provides up to 16 million tunnels in the same administrative domain.

VxLAN creates LAN segments using MAC Address-in-User Datagram Protocol (MAC-in-UDP) encapsulation.

Figure 1-7 shows VLANs 32 and 47 connected by a VxLAN tunnel named VNID 82.VTEP-14 routes packets from VLAN 32 to the transport network based on the IP address of VTEP-37. VTEP-37 receives the packets, strips the outer headers, and forwards the packets to a host identified by the destination MAC address on VLAN 47.

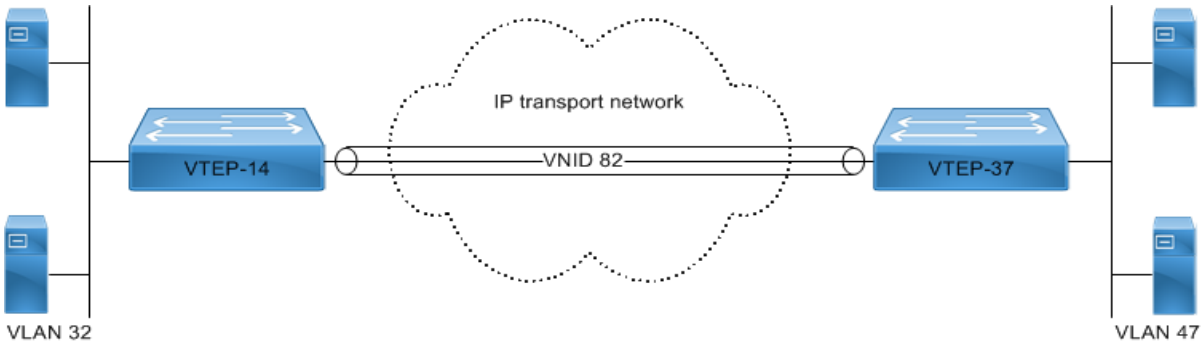


Figure 1-7: VxLAN High-level Architecture

VxLAN EVPN using MP-BGP

OcNOS supports VxLAN EVPN (Ethernet Virtual Private Network) using MP-BGP where the virtual machine MAC address learning happens in the control plane using MP-BGP and not in the data plane. This allows dynamic learning and provisioning of tunnels and hosts. BGP route reflectors can be deployed on the carrier backbone network. All provider edge devices maintain a peer relationship with the BGP route reflectors. The route reflectors distribute the EVPN routes.

SECTION 2 System Management

System Management Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 User Configuration

Overview

User management is an authentication feature that provides administrators with the ability to identify and control the users who log into the network.

OcNOS provides 4 different roles for users.

- Network Administrator: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Operator: can make permanent changes to switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: displays information; cannot modify configuration.

User Configuration

`#configure terminal`	Enter configure mode.
`(config)#username user1 password user12345`	Create Username “user1” with password user12345 which will have default role as network-user. Password should be <8-32> char, username <2-15>char.
`(config)#username user1 role network-operator password user12345`	Changing the role for user1 to network-operator. Password should be <8-32> char, username <2-15>char.
`(config)#username user2 role network-operator password user12345`	Create a user “user2” with role as network-operator. Password should be <8-32> char, username <2-15>char.
`(config)#username user3 role network-admin password user12345`	Create a user “user3” with role as network-admin. Password should be <8-32> char, username <2-15>char.
`(config)#username user4 role network-engineer password user12345`	Create a user “user4” with role as network-engineer. Password should be <8-32> char, username <2-15>char.
`(config)#exit`	Exit configure mode.

Validation

show user-account, show user-account <username>, show role

```
#show user-account
User:user1
                roles: network-operator
User:user2
                roles: network-operator
User:user3
                roles: network-admin
User:user4
                roles: network-engineer
```

```
#show role
Role Name                                Info
------------------------------------------------------------------------
network-admin          Network Administrator - Have all permissions
network-engineer       Network Engineer - Can save configuration
network-operator       Network Operator - Can not save configuration
network-user           Network User - Can not change configuration
rbac-customized-role   RBAC User - Can change only  permitted configuration

#show user-account user1
User:user1
                roles: network-operator
```

CHAPTER 2 Using the Management Interface

Overview

OcNOS provides support for different types of Management Interfaces. The management interface can be the standard out of band (OOB) port, or any in-band port.

To provide segregation between management traffic and data traffic, OcNOS provides a Management VRF. The Management VRF is created by default when OcNOS boots. This VRF cannot be deleted. All ports used as Management Interface needs to be in Management VRF. The management VRF is used for all types of Management applications listed below

- Remote access to router (SSH/Telnet)
- File transfer applications (SFTP/SCP)
- Login Authentication via Radius/Tacacs
- Network management protocols (SNMP, Netconf)

Apart from this, DHCP, DNS, NTP, Syslog, License/Software upgrade also uses ports mapped to management VRF for their operations. Also LLDP protocol can be run on any ports mapped to this Management VRF.

Note: If the management interface flaps, the device becomes unreachable.

Management Port

The Out of Band (OOB) Management Port in OcNOS is identified as “eth0.” This port is automatically mapped to the Management VRF when OcNOS boots, and will remain in same VRF throughout. It cannot be moved out of this VRF.

The IP address of the management port can be configured statically or via DHCP.

Static IP Configuration

A static IP can be configured on the management port during ONIE installation itself, or after installation using the OcNOS CLIs commands. To configure a static IP during ONIE installation, do the following

```
#onie-discovery-stop
#ifconfig eth0 <ip address> netmask <subnet mask> up
```

Please check the Install Guide for details.

The IP address configured during ONIE installation will be applied to the management port and the same will be retained when OcNOS boot up, and the port becomes part of Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address 10.12.44.109/24
```

After getting the OcNOS prompt, this IP address can be changed from the CLI.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address 10.12.44.120/24`	Assign an IPv4 address to the interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configure mode

If a static IP is not configured during ONIE installation the same can be configured via CLI by following the above steps. Using the OcNOS CLI, DHCP can also be enabled on the Management port.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address dhcp`	Enable DHCP on interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configure mode

Obtaining IP Address via DHCP

During onie installation, the management port attempts to acquire IP address via DHCP automatically unless stopped explicitly using “onie-discovery-stop”. So, if management port is getting IP via DHCP, after OcNOS boots, the management port will continue to use DHCP, even when it is part of the Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
```

After OcNOS boots, the IP address can be changed to any static IP from the command line as shown earlier.

In-Band Ports

Any front-end ports of the device (in-band ports) can be made part of the management VRF. Once they are part of the management VRF they can also support all management applications such as SSH/Telnet and others as listed in Overview.

Once the ports are part of the management VRF, they should not be used for data traffic and routing or switching purposes. In-band ports can be added or removed from Management VRF as and when required.

`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode
`(config-if)#ip vrf forwarding management`	Add in-band port to Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configure mode

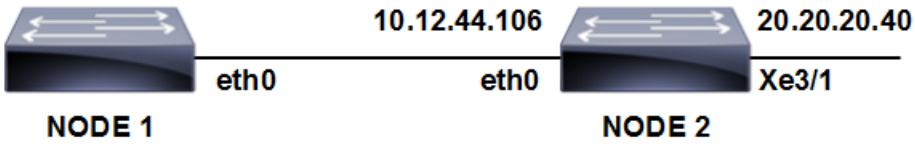
`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode

`(config-if)# no ip vrf forwarding management`	Remove in-band port from Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configure mode

Using Ping in Management VRF

To check reachability to any node in the management network, you need to explicitly mention the VRF name as “management.”

In the following example, Node-1 has management interface eth0 and Node-2 has management interfaces eth0 and xe3/1. In order to reach the network 20.20.20.40/24 from Node-1 a static route needs to added.



`#configure terminal`	Enter configure mode
`(config)# ip route vrf management 20.20.20.0/24 10.12.44.106 eth0`	Add static route in management VRF to reach 20.20.20.0/24 network
`(config)#exit`	Exit configure mode

```
Node-1#show ip route vrf management
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "management"
C       10.12.44.0/24 is directly connected, eth0
S       20.20.20.0/24 [1/0] via 10.12.44.106, eth0

Gateway of last resort is not set

Node-1#ping 20.20.20.40 vrf management
PING 20.20.20.40 (20.20.20.40) 56(84) bytes of data.
64 bytes from 20.20.20.40: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 20.20.20.40: icmp_seq=2 ttl=64 time=0.476 ms
```

CHAPTER 3 SSH Client Server Configuration

Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model

TCP port 22 is assigned for contacting SSH servers. This document covers the SSH server configuration to enable SSH service and key generation and SSH client configuration for remote login to server.

In-band Management over Default VRF

OcNOS supports SSH over the default and management VRFs via the in-band management interface and out-of-band management interfaces, respectively.

SSH can run on the default and management VRFs simultaneously. By default, it runs on the management VRF.

Topology

Figure 3-8: SSH sample topology

Basic Configuration

`#configure terminal`	Enter configure mode
`(config)#ssh login-attempts 2 vrf management`	Set the number of login attempts to 2
`(config)#exit`	Exit configure mode

Validation

```
#show ssh server
ssh server enabled port: 22
authentication-retries 2

#show running-config ssh server
feature ssh vrf management
ssh login-attempts 2 vrf management
```

SSH Client Session

When the device acts as an SSH client, it supports both SSH IPv4 sessions to log into the remote machine.

`#ssh root@10.10.10.1 vrf management`	Log into remote machine using an IPv4 address

SSH Keys

Use the ssh key command to generate new RSA/DSA keys for the SSH server. By default, the system has RSA/DSA public/private key pair placed in `/etc/ssh/`. If you want to regenerate RSA keys, you must specify the `force` option.

Configuration

`#configure terminal`	Enter configure mode.
`(config)#ssh key rsa force vrf management`	Specify the `force` option to regenerate SSH RSA keys
`(config)#exit`	Exit configure mode

Validation

```
#sh ssh key
****************RSA KEY********************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj
bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48
************************************
****************DSA KEY********************
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
```

```
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=
bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
************************************
```

Note: The newly created rsa/dsa key can be verified by logging into the device from a remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

SSH Encryption Cipher

Specify an SSH cipher to encrypt an SSH session. By default, all the ciphers are supported for a new SSH client to connect to the SSH server.

SSH supports these encryption algorithms:

- Advanced Encryption Standard Counter:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
- Advanced Encryption Standard Cipher Block Chaining:
  - aes192-cbc
  - aes256-cbc
- Triple Data Encryption Standard Cipher Block Chaining:
  - 3des-cbc

Configuration

`#configure terminal`	Enter configure mode
`(config)#ssh server algorithm encryption aes128-ctr vrf management`	Set the SSH server encryption algorithm to AES 128 bit counter
`(config)#ssh server algorithm encryption aes128-cbc vrf management`	Set the SSH server encryption algorithm to AES 128 cipher block chaining
`(config)#exit`	Exit configure mode

Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config ssh server
feature ssh vrf management
ssh server algorithm encryption aes128-ctr aes128-cbc vrf management
```

SSH Client Session

`#ssh cipher aes128-ctr root@1.1.1.1 vrf management`	Specify AES 128-bit counter encryption to establish an SSH connection to a remote machine using an IPv4 address

SSH Key-Based Authentication

Enable OcNOS device SSH server to perform public key based SSH authentication, to enable machine to machine communication possible without requiring password. Public key based authentication increases the trust between two Linux servers for easy file synchronization or transfer. Public-key authentication with SSH is more secure than password authentication, as it provides much stronger identity checking through keys.

Topology

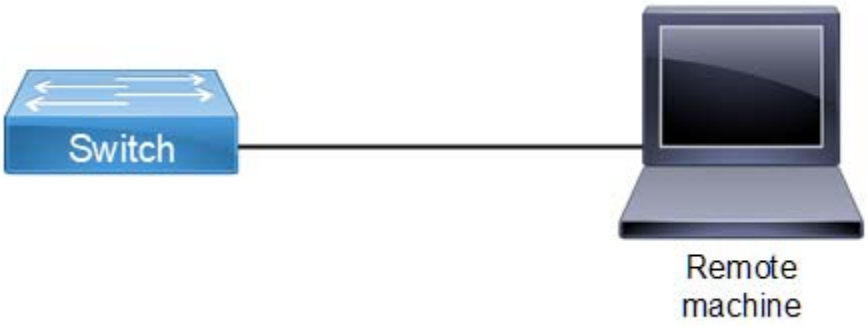


Figure 3-9: SSH Key-based authentication

Public Key Authentication Method

The server has the public key of the user stored; using this the server creates a random value, encrypts it with the public key and sends it to the user. If the user is who is supposed to be, he can decrypt the challenge using the private key and send it back to the server, server uses the public key again to decrypt received message to confirm the identity of the user. SSH is supported in-band (default VRF) and out of band (management VRF). Installed keys are stored in the `~/.ssh/authorized_keys` file.

SSH key based authentication steps:

1. Login to remote machine Linux desktop (ssh client) and generate the key pair using the `ssh-keygen` command.
2. Create the username in OcNOS device (ssh server).
3. Install the public key of remote Linux ssh client in the OcNOS device.
4. Display the installed key in the OcNOS device using the `show running-config` command.
5. Log in from the remote Linux ssh client to the OcNOS device without providing a password.

Useful Commands on Remote Desktop Client

`# ssh-keygen`	To generate key pair on remote Linux machine (ssh client)
`# cd /bob/.ssh/`	To go to the location of saved key pair
`# cat id_rsa.pub`	Command to display the generated public key in remote Linux client

Configuration commands in OcNOS

`#configure terminal`	Enter configure mode.
`#feature ssh vrf management`	Enable the SSH feature on vrf management. To enable in default vrf give the command "feature ssh"
`#username fred`	To create username with default role as network-user. To create user with different role specify role using command "username <username> role <role_name>
`#username fred sshkey AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/VHVgU2Y0/ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain`	Install the public key of remote Linux client in OcNOS device.
`#exit`	Exit configure mode.

Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config

<skipped other content>
feature ssh vrf management
username fred role network-user
username fred sshkey
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
<skipped other content>
#show running-config ssh server
feature ssh vrf management
```

SSH Key-based Client Session

`#ssh fred@10.10.26.186`	Specify user name and ip address to access the device. Supports IPv4 and IPv6.User should be able to access without password and through key based authentication

Restrictions

- Key generation or installation are not supported for "root" user account in OcNOS device.
- Third party SSH utilities cannot be used for key installation, rather OcNOS CLI is the only way to install public keys.

Sample Use Case

1. Login to remote machine linux desktop (ssh client) and generate the key pair using the `ssh-keygen` command.

```
[bob@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/bob/.ssh/id_rsa):
/bob/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /bob/.ssh/id_rsa.
Your public key has been saved in /bob/.ssh/id_rsa.pub.
The key fingerprint is:
b2:d0:cc:d2:dd:db:3d:05:c1:33:fc:4a:df:8e:85:af bob@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|             o.  |
|              =. |
|              .+ |
|     = . .    ...|
|    o * S .  . +o|
|     o o   o .o.+|
|      .   . . o= |
|              ..o|
|              E. |
+-----------------+
[bob@localhost ~]# cd /bob/.ssh/
[bob@localhost .ssh]# cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
[bob@localhost .ssh]#
```

2. Create username in OcNOS switch device (ssh server)

```
(config)#username fred
```

Note: By default, the user role is `network-user`.

3. Install the public key of remote Linux ssh client in OcNOS device.

```
(config)#username fred sshkey
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
```

4. Display the installed key in OcNOS device using the `show running-config` command.

```
#show running-config
<skipped other content>
username fred role network-user
username fred sshkey
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
<skipped other content>
```

5. Login from remote Linux ssh client to OcNOS device without providing password

```
[bob@localhost .ssh]# ssh fred@10.10.26.186
```

CHAPTER 4 Telnet Configuration

Overview

Telnet is a TCP/IP protocol used on the Internet and local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. The Telnet program runs, connects it to a server on the network. A user can then enter commands through the Telnet program and they will be executed as if the user were entering them directly on the server console.Telnet enables users to control the server and communicate with other servers on the network. The default port number for Telnet protocol is 23.Telnet offers users the capability of running programs remotely and facilitates remote administration.

Support for In-band Management Over Default VRF

OcNOS supports Telnet over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, Telnet runs on the management VRF.

Topology

Figure 4-10: Telnet topology

Enable and Disable the Telnet Server

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#telnet server port 6112 vrf management`	Set Telnet port to 61112
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#exit`	Exit configure mode

Telnet Client Session

`#telnet 10.10.10.1 vrf management`	Log into remote machine using IPv4 address

Validation Commands

```
#show telnet server
telnet server enabled port: 6112

#show running-config telnet server
feature telnet
```

CHAPTER 5 Syslog Configuration

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate, a means to notify administrators of problems or performance.

OcNOS supports logging messages to a syslog server in addition to logging to a file or the console (local or ssh/telnet console). OcNOS messages can be logged to a local syslog server (the machine on which OcNOS executes) as well as to one or more remote syslog servers. Remote syslog servers can either be configured with IPv4 addresses or host names.

Support for In-band management over default VRF

OcNOS supports syslog over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, syslog runs on the management VRF.

Topology

Figure 5-11: Syslog sample topology

Enabling rsyslog

`#configure terminal`	Enter configure mode.
`config)#feature rsyslog [vrf management]`	Enable feature on default or management VRF. By default this feature runs on the management VRF.
`config)#exit`	Exit configure mode

Logging to a File

The below configurations shows how to enable debug logs for a particular protocol. In this case, OSPF is shown.

`#debug ospf all`	This enables the debugging on OSPF.
`#configure terminal`	Enter configure mode
`(config)#router ospf 1`	Enable OSPF process 1

(config-router)#exit	Exit router mode
(config)#feature rsyslog	Enable feature on default or management VRF. By default this feature runs on the management VRF.
(config)#logging level ospf 7	This enable debug messages for OSPF module. This is configurable either if default of management VRF.
(config)#logging logfile ospf1 7	This creates the log file where the logs will be saved. The path of the file will be in the directory /log/ospf1. Log File size 4096-4194304 bytes.
(config)#exit	Exit configure mode

To verify this, do some OSPF configuration and view the messages in the log file or with the `show logging logfile` command.

Validation Commands

```
    #show logging logfile

    File logging : enabled  File Name : /log/ospf1  Size : 419430400  Severity :
    (7)
    2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO : NSM Message Header
    2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO :  VR ID: 0
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  VRF ID: 0
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message type:
    NSM_MSG_LINK_ADD
     (5)
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message length: 232
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message ID: 0x00000000
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : NSM Interface
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Interface index: 100001
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Name: po1
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Flags: 536875010
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Status: 0x00000804
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Metric: 1
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  MTU: 1500
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  Type: L3
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  HW type: 9
    2019 Jan 05 20:10:52.208 : OcNOS : OSPF : INFO :  HW len: 6
    2019 Jan 05 20:10:52.209 : OcNOS : OSPF : INFO :  HW address: ecf4.bb5c.a2b0
    2019 Jan 05 20:10:52.210 : OcNOS : OSPF : INFO :  Bandwidth: 0.000000
    2019 Jan 05 20:10:52.211 : OcNOS : OSPF : INFO :  Interface lacp key flag 0
    2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO :  Interface lacp aggregator
    upda
    te flag 0

#show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                       3
    ripd                    3                       3
    ospfd                   3                       7
    ospf6d                  3                       3
    isisd                   3                       3
    hostpd                  3                       3
    ldpd                    2                       2
    rsvpd                   2                       2
```

```
    mribd                   2                       2
    pimd                    2                       2
    authd                   2                       2
    mstpd                   2                       2
    imi                     2                       2
    onmd                    2                       2
    oamd                    2                       2
    vlogd                   2                       2
    vrrpd                   2                       2
    ribd                    2                       2
    bgpd                    3                       3
    l2mribd                 2                       2
    lagd                    2                       2
    sflow                   2                       2
    pservd                  2                       2
```

Logging to the Console

`#configure terminal`	Enter configure mode.
`(config)#logging level ospf 7`	This enable debug messages for OSFP module.
`(config)#logging console 7`	This enables the console logs.
`(config)#debug ospf`	This enables the debugging on OSPF configurations.
`(config)#router ospf`	Enabling ospf for process 1.
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit configure mode.

To verify this, do some OSPF configuration and view the messages in the console.

Validation Commands

```
#show logging console
    Console logging     : enabled Severity: (debugging)

#show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                       3
    ripd                    3                       3
    ospfd                   3                       7
    ospf6d                  3                       3
    isisd                   3                       3
    hostpd                  3                       3
    ldpd                    2                       2
    rsvpd                   2                       2
    mribd                   2                       2
    pimd                    2                       2
    authd                   2                       2
    mstpd                   2                       2
    imi                     2                       2
    onmd                    2                       2
    oamd                    2                       2
```

```
    vlogd                   2                               2
    vrrpd                   2                               2
    ribd                    2                               2
    bgpd                    3                               3
    l2mribd                 2                               2
    lagd                    2                               2
    sflow                   2                               2
    pservd                  2                               2
```

Logging to Remote Server

`#configure terminal`	Enter configure mode.
`(config)#logging level bgp 7`	This enable debug messages for BGP module.
`(config)#logging server 10.16.2.1 vrf management`	Redirects the log messages to the server configured.
`(config)#debug bgp`	This enables the debugging on BGP configurations.
`(config)#router bgp 1`	Enabling BGP process 1.
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit configure mode.

Validation Commands

```
#show logging server
      Remote Servers:
                  10.16.2.1
                  severity: (debugging)
                  facility: local7
                  VRF: management

    #show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                               3
    ripd                    3                               3
    ospfd                   3                               3
    ospf6d                  3                               3
    isisd                   3                               3
    hostpd                  3                               3
    ldpd                    2                               2
    rsvpd                   2                               2
    mribd                   2                               2
    pimd                    2                               2
    authd                   2                               2
    mstpd                   2                               2
    imi                     2                               2
    onmd                    2                               2
    oamd                    2                               2
    vlogd                   2                               2
    vrrpd                   2                               2
    ribd                    2                               2
    bgpd                    3                               7
```

```
l2mribd                 2                       2
lagd                    2                       2
sflow                   2                       2
pservd                  2                       2
```

CHAPTER 6 DNS Configuration

Overview

The Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. When a domain name is used, DNS service translates the name into the corresponding IP address. If one DNS server does not know how to translate a particular domain name, it gathers information from other Domain Name Systems to obtain the correct IP address.

Support for In-band Management over default VRF

OcNOS offers support for DNS over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on management VRF.

Topology

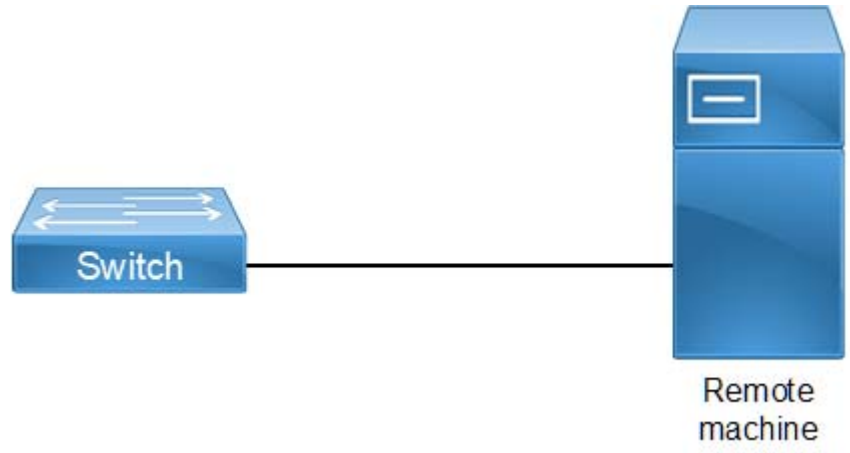


Figure 6-12: DNS sample topology

Configuration

`#configure terminal`	Enter Configure mode.
`(config)#ip name-server vrf management 10.12.17.11 10.1.1.2`	This add a IPv4 Name Server to the DNS.
`(config)#ip host BINGO vrf management 10.1.1.1`	This will add IPv4 host to the DNS
`(config)#exit`	Exit configure mode.

Validation Commands

```
#show hosts
```

```
         VRF: default

 DNS lookup is disabled
 Default domain is empty
 DNS domain list is empty

 Name Servers        : 10.12.17.11 10.1.1.2
Host                                                                Address

----                                                                -------

BINGO                                                               10.1.1.1


 * - Values assigned by DHCP Client.
```

CHAPTER 7 DHCP Client Configuration

Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

DHCP Client Configuration for IPv4

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

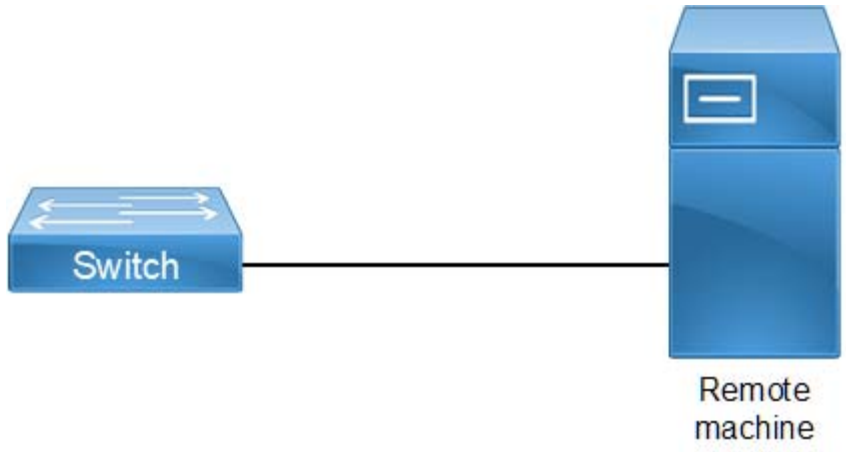


Figure 7-13: DHCP sample topology

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#interface eth0`	Enter management interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#show running-config dhcp
    interface xe2
     ip address dhcp
    !
    ip dhcp relay information option

    #sh ip interface brief

    Interface           IP-Address     Admin-Status         Link-Status
    GMPLS Type
    eth0                10.12.44.20     up                  up
    -
    lo                  127.0.0.1       up                  up
    -
    lo.4                127.0.0.1       up                  up
    -
    vlan1.1             unassigned      up                  down
    -
    xe1/1               2.2.2.3         up                  up
    -
    xe1/2               unassigned      down                down
    -
    xe1/3               unassigned      down                down
    -
    xe1/4               unassigned      up                  down
    -
    xe2                *40.40.40.40     up                  down
    -
    xe3/1               20.20.30.1      up                  up
    -
```

CHAPTER 8 Software Monitoring and Reporting

Overview

OcNOS provides a mechanism (called “watchdogging”) to monitor all OcNOS modules and provides the following functions.

1. Periodic heart beat check.
2. Automatic restarts of a module upon a hung state or crash detection.
3. Upon hanging or crashing of a module, a crash report (including system states) is logged.
4. A proprietary SNMP trap is sent to the trap manager, if configured, after a fault is detected in a protocol module. Similarly a trap is sent when the module recovers.

By default, the software watchdog is enabled and the keep-alive time interval is 30 seconds. All OcNOS processes periodically send keep-alive messages to a monitoring module at the configured keep-alive time interval.

This functionality can be disabled for a particular module or all OcNOS modules by using CLI commands. In order to permanently disable software monitoring functionality, the user has to disable the watchdog feature. If, however, software watchdogging is disabled the monitoring module doesn’t take any action upon a hang or crash of any OcNOS module.

Software Monitoring

`#configure terminal`	Enter Configure mode.
`(config)#feature software-watchdog`	Enable software watchdog for all OcNOS modules — This is the default.
`(config)#no software-watchdog imi`	To disable software watchdog for only imi modules.
`(config)#software-watchdog keep-alive-time 100`	The keep-alive time interval in seconds. Default is 60 seconds and applies to all OcNOS modules.
`#show software-watchdog status`	Display the keep-alive time interval and list of OcNOS process names with watchdog status for each OcNOS modules.

Validation

```
#show software-watchdog status
Software Watchdog timeout in seconds : 100
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ospfd                Enabled
isisd                Enabled
hostpd               Enabled
ldpd                 Enabled
rsvpd                Enabled
```

```
mribd               Enabled
pimd                Enabled
authd               Enabled
mstpd               Enabled
imi                 Disabled
onmd                Enabled
HSL                 Enabled
oam                 Enabled
vlogd               Enabled
vrrpd               Enabled
ndd                 Enabled
ribd                Enabled
bgpd                Enabled
l2mribd             Enabled
lagd                Enabled
sflow               Enabled
```

CHAPTER 9 TACACS Client Configuration

Overview

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device. TACACS+ listens at port 49.

TACACS Server Authentication

Figure 9-14: TACACS Server Host Configuration

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for management vrf
`(config)#feature tacacs+`	Enable the feature TACACS+. for default vrf
`(config)#tacacs-server login key testing101 vrf management`	Specify the global key for tacacs servers that are not configured with their respective keys for management vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login key testing101`	Specify the global key for tacacs servers that are not configured with their respective keys for default vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login host 10.16.19.2 vrf management key testing123`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file
`(config)#tacacs-server login host 10.16.19.2 key testing123`	Specify the tacacs server ipv4 address to be configured with shared local key for default vrf The same key should be present on the server config file.
`(config)#tacacs-server host 10.12.30.86 vrf management seq-num 2 port 1045`	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
`config)#tacacs-server login host 10.12.30.86 seq-num 2 port 1045`	Specify the tacacs server ipv4 address to be configured with the sequence and port number for default vrf. The tacacs server should be started with same port number
`(config)#tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port 65535`	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for management vrf. The tacacs server should be started with same port number.

`(config)#tacacs-server login host 10.12.17.11 seq-num 8 key 7 65535 port 65535`	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for default vrf. The tacacs server should be started with same port number.
`(config)#tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535`	Specify the tacacs server configured with host-name sequence number key and port number for management vrf. The tacacs server should be started with same port number
`(config)#tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 65535`	Specify the tacacs server configured with host-name sequence number key and port number for default vrf. The tacacs server should be started with same port number
`(config)#aaa authentication login default vrf management group tacacs+`	Enable authentication for TACACS+ server configured for management vrf. Authorization is also enabled by default
`(config)#aaa authentication login default group tacacs+`	Enable authentication for TACACS+ server configured for default vrf. Authorization is also enabled by default.
`(config)#aaa authentication login default vrf management group tacacs+ local`	Enable authentication for TACACS+ and fall-back to local configured for management vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group tacacs+ local none`	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for management vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group tacacs+ none`	Enable authentication for TACACS+ fall-back to none configured for management vrf. Authorization is also enabled by default
`(config)#aaa authentication login default group tacacs+ none`	Enable authentication for TACACS+ fall-back to none , configured for default vrf. Authorization is also enabled by default
`(config)#aaa group server tacacs+ G1 vrf management`	Create aaa group G1 for management vrf
`(config-tacacs)#server 10.12.30.86 vrf management`	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
`(config-tacacs)#server Tacacs-Server-1`	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
`(config-tacas)#exit`	Exit the tacacs-config
`(config)#aaa group server tacacs+ G1`	Create aaa group G1 for default vrf
`(config-tacacs)server 10.12.30.86`	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
`(config-tacacs)#server Tacacs-Server-1`	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
`(config-tacacs)#exit`	Exit the tacacs-config mode
`(config)#aaa authentication login default vrf management group G1`	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
`(config)#aaa authentication login default group G1`	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

Users are mapped as shown as shown in Table 9-1:

Table 9-1: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14

Table 9-1: Role/privilege level mapping (Continued)

Role	Privilege level
Network operator	1 to 13
Network user	0 or any other values (>15 or negative values or any character)

Validation

```
Leaf1#show tacacs-server vrf management
        VRF: management
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.30.86/1045
           Sequence Number      : 2
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-Server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Leaf1#show tacacs-server
        VRF: default
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.30.86/1045
           Sequence Number      : 2
      Failed Auth Attempts      : 0
```

```
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    Tacacs+ Server                 : Tacacs-Server-1/65535
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    Tacacs+ Server                 : 10.12.17.11/65535
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs-server vrf all
             VRF: management
    total number of servers:2
    Tacacs+ Server                 : Tacacs-Server-1/65535(*)
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                 : 10.12.17.11/65535
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:


             VRF: default
    total number of servers:2

    Tacacs+ Server                 : Tacacs-Server-1/2222
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    Tacacs+ Server                 : 100.0.0.1/2222
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:


    (*) indicates last active.
```

```
#


    #
#show tacacs-server
            VRF: default
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs-server vrf management groups G1
            VRF: management

            group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 65535
                    key is ********

                    server 10.12.17.11:
                    seq-num 8
                    port is 65535
                    key is ********

#show tacacs-server vrf all groups G1
            VRF: management

            group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 65535
                    key is ********

                    server 10.12.17.11:
                    seq-num 8
                    port is 65535
                    key is ********


            VRF: default

            group G1:
```

```
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 2222
                    key is ********

                    server 100.0.0.1:
                    seq-num 8
                    port is 2222
                    key is ********



#
#show tacacs-server groups G1
            VRF: default
    group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 2222
                    key is ********

                    server 100.0.0.1:
                    seq-num 8
                    port is 2222
                    key is ********
    #show tacacs vrf management
            VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
               Sequence Number      : 7
         Failed Auth Attempts       : 0
        Success Auth Attempts       : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
               Sequence Number      : 8
         Failed Auth Attempts       : 0
        Success Auth Attempts       : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.



    #show tacacs vrf all
            VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
               Sequence Number      : 7
         Failed Auth Attempts       : 0
        Success Auth Attempts       : 1
       Failed Connect Attempts      : 0
```

```
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


(*) indicates last active.
#

#show tacacs
        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs vrf management
        VRF: management
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/65535(*)
           Sequence Number      : 7
```

```
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                 : 10.12.17.11/65535
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs vrf all
            VRF: management
    total number of servers:2

    Tacacs+ Server                 : Tacacs-Server-1/65535(*)
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                 : 10.12.17.11/65535
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:


            VRF: default
    total number of servers:2

    Tacacs+ Server                 : Tacacs-Server-1/2222(*)
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                 : 100.0.0.1/2222
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:


    (*) indicates last active.
#

#show tacacs
            VRF: default
```

```
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222(*)
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show aaa authentication vrf management
                     VRF: management
      default: group G1
      console: local

#show aaa authentication vrf all
                     VRF: management
      default: group G1
      console: local

                     VRF: default
      default: group tacacs+
      console: local

#show aaa authentication
                     VRF: default
      default: group tacacs+
      console: local
#

# show aaa groups vrf management
                     VRF: management
    radius
    tacacs+
    G1

#
    # show aaa groups vrf all
                     VRF: management
    radius
    tacacs+
    G1

                     VRF: default
    radius
    tacacs+
    G1
```

```
#show aaa groups
                    VRF: default
    radius
    tacacs+
    G1

#show running-config tacacs+
    feature tacacs+ vrf management
    tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535
    po
    rt 65535
    tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port
    6
    5535

    feature tacacs+
    tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 2222
    tacacs-server login host 100.0.0.1 seq-num 8 key 7 65535 port 2222

#show running-config aaa
    aaa authentication login default vrf management group G1
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1

#show running-config aaa all
    aaa authentication login default vrf management group G1
    aaa authentication login console local
    aaa accounting default vrf management local
    no aaa authentication login default fallback error local vrf management
    no aaa authentication login console fallback error local
    no aaa authentication login error-enable vrf management
    aaa local authentication attempts max-fail 3
    aaa local authentication unlock-timeout 1200
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa authentication login console local
    aaa accounting default local
    no aaa authentication login default fallback error local
    no aaa authentication login console fallback error local
    no aaa authentication login error-enable
    aaa local authentication attempts max-fail 3
    aaa local authentication unlock-timeout 1200
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1
```

TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for vrf management
`(config)#feature tacacs+`	Enable the feature TACACS+ for default vrf
`(config)#tacacs-server host 10.16.19.2 vrf management key testing123`	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
`(config)#tacacs-server login host 10.16.19.2 key testing123`	Specify the TACACS server IPv4 address to be configured with shared key default vrf. The same key should be present in the server configuration file.
`(config)#aaa accounting default vrf management group tacacs+`	Enable accounting for TACACS server configured for vrf management.
`(config)#aaa accounting default group tacacs+`	Enable accounting for TACACS server configured for default vrf
`(config)#exit`	Exit configure mode
`#clear tacacs-server counters vrf management`	Clear tacacs server counters for management vrf
`#clear tacacs-server counters vrf all`	Clear tacacs server counters for management and default vrf
`#clear tacacs-server counters`	Clear tacacs server counters for default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting vrf management
                     VRF: management
          default: group tacacs+
#

#show aaa accounting vrf all
                     VRF: management
          default: group tacacs+

                     VRF: default
          default: group tacacs+

#show aaa accounting
```

```
                    VRF: default
          default: group tacacs+
          #

#show running-config aaa
    aaa authentication login default vrf management group G1
    aaa accounting default vrf management group tacacs+
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa accounting default group tacacs+
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1
```

Sample TACACS Config File Contents

```
#tacacs configuration file
#set the key

    key = "testing123"
    accounting file = /var/log/tac_acc.log

    user = test1 {
            default service = permit
            login = cleartext "12345"
    }

    group = netadmin {
            service = ppp protocol = ip {
            priv-lvl = 1
            }
    }

    user = test2 {
            default service = permit
            login = cleartext "12345"
            member = netadmin
    }

    user = test3 {
            default service = permit
            login = cleartext "12345"
            service = ppp protocol = ip {
            priv-lvl = 15
    }
    }
```

TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in Table 9-1.

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in Table 9-1.

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level <=0 and priv-level > 15 are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is “auto-enabled”. After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configure mode. An error message is displayed upon executing any command which is not allowed.

```
#write
% Access restricted for user %
#configure terminal
% Access restricted for user %
```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```
service = ppp protocol = ip {
        priv-lvl = <0…15>
}
```

Sample TACACS+ Configuration File

```
#tacacs configuration file from “tac_plus version F4.0.3.alpha “
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user “test1”, without any priv-lvl, mapped to role “network-user”
user = test1 {
default service = permit
login = cleartext "12345"
}

#We can create a group of users mapped to a privilege
group = netadmin {
service = ppp protocol = ip {
priv-lvl = 15
}
}

#User “test2” with highest priv-lvl=15, mapped to role “network-admin”
user = test2 {
default service = permit
login = cleartext "12345"
```

```
member = netadmin
}

#User “test3” with priv-lvl= 1…13, mapped to role “network-operator”
user = test3 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 10
}
}
#User “test4” with priv-lvl=14, mapped to role “network-engineer” user = test4 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 14
}
}
```

CHAPTER 10 RADIUS Client Configuration

Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server.

A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

The key points for RADIUS authentication are:

- Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
- The password is encrypted before sending it over the network.

RADIUS Server Authentication

Figure 10-15: RADIUS Server Host Configuration

Host

`#configure terminal`	Enter configure mode.
`(config)# radius-server login key testing101 vrf management`	Specify the global key for radius servers that are not configured with their respective keys for management vrf. This key should match the one present in the config file of tacacs server.
`(config)# radius-server login key testing101`	Specify the global key for radius servers that are not configured with their respective keys for default vrf. This key should match the one present in the config file of tacacs server
`(config)# radius-server login host 10.12.17.13 vrf management key testing123`	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
`(config)# radius-server login host 10.12.17.13 key testing123`	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.
`(config)# radius-server login host 10.12.17.11 vrf management auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for management vrf. The radius server should be started with same port number.

`(config)# radius-server login host 10.12.17.11 auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for default vrf. The radius server should be started with same port number. The radius server should be started with same port number
`(config)#radius-server login host Radius-Server-1 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2`	Specify the radius server configured with hostname, key authentication port number, accounting port number, for management VRF. The radius server should be started with same port number
`radius-server login host Radius-Server-1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2`	Specify the radius server configured with hostname sequence number, key and port number for default VRF. The radius server should be started with same port number.
`(config)#aaa authentication login default vrf management group radius`	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius`	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.
`(config)#aaa authentication login default vrf management group radius local`	Enable authentication for radius server and fallback to local configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius local`	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group radius local none`	Enable authentication for radius server, fallback to local followed by fallback to none, configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default radius local none`	Enable authentication for radius server, fallback to local followed by fallback to none, configured for default vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group radius none`	Enable authentication for radius, fallback to none, configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius none`	Enable authentication for radius, fallback to none, configured for default VRF. Authorization is also enabled by default
`(config)#aaa group server radius G1 vrf management`	Create aaa radius group G1 for management vrf
`(config)#aaa group server radius G1`	Create AAA radius group G1 for default VRF
`(config-radius)#server 10.12.30.86`	Make the radius server 10.12.30.86 a part of this group G1 for default VRF
`(config-radius)#server Radius-Server-1`	Make Radius-Server-1 a part of this group G1
`(config-radius)#exit`	Exit radius mode
`(config)#aaa group server radius G1`	Enter radius mode
`(config-radius)#server 10.12.30.86`	Make the radius server 10.12.30.86 a part of this group G1 for default vrf
`(config-radius)#server Radius-Server-1`	Make Radius-Server-1 a part of this group G1
`(config)#exit`	Exit radius mode.

`(config)#aaa authentication login default vrf management group G1`	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
`(config)#aaa authentication login default group G1`	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

Validation

To verify the RADIUS authentication process, use SSH or Telnet from the host machine to Host IP with the authenticating user created, and provide a RADIUS server password and check whether the client validates the user with the corresponding username and password.

```
#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                           : 10.12.17.13
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 2
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:55:44
Radius Server                           : 10.12.17.11 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:58:33

#show radius-server
        VRF: default
timeout value: 5

Total number of servers:4

Following RADIUS servers are configured:
Radius Server                           : 192.168.1.1
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 1
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:45:09
```

```
Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:46:36

#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                           : 10.12.17.13
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 2
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:55:44
Radius Server                           : 10.12.17.11 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:58:33

#show radius-server
        VRF: default
timeout value: 5

Total number of servers:4

Following RADIUS servers are configured:
Radius Server                           : 192.168.1.1
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
```



```
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 1
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:45:09

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:46:36

#show radius-server vrf all
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                           : 10.12.17.13
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 2
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:55:44
Radius Server                           : 10.12.17.11 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:58:33

        VRF: default
timeout value: 5

Total number of servers:4
```

```
Following RADIUS servers are configured:
Radius Server                          : 192.168.1.1
   Sequence Number                     : 1
   available for authentication on port : 60000
   available for accounting on port    : 60000
   timeout                             : 2
   RADIUS shared secret                : ********
   Failed Authentication count         : 0
   Successful Authentication count     : 1
   Failed Connection Request           : 2
   Last Successful authentication      : 2000 January 05, 20:45:09

Radius Server                          : 100.0.0.1 (*)
   Sequence Number                     : 2
   available for authentication on port : 60000
   available for accounting on port    : 60000
   timeout                             : 2
   RADIUS shared secret                : ********
   Failed Authentication count         : 1
   Successful Authentication count     : 1
   Failed Connection Request           : 0
   Last Successful authentication      : 2000 January 05, 20:46:36

#show running-config radius
radius-server login key 7 0x6f32ba3f9e05a3db vrf management
radius-server login host 10.12.17.13 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb

#show running-config aaa
aaa authentication login default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1

#show running-config aaa all
aaa authentication login default vrf management group radius
aaa authentication login console local
aaa accounting default vrf management local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa authentication login console local
aaa accounting default local
no aaa authentication login default fallback error local
no aaa authentication login console fallback error local
```

```
    no aaa authentication login error-enable
    aaa local authentication attempts max-fail 3
    aaa local authentication unlock-timeout 1200
    aaa group server radius rad1
        server Radius-Server-1
        server 100.0.0.1
```

RADIUS Server Accounting

You can configure accounting to measure the resources that another user consumes during access.

User

`#configure terminal`	Enter configure mode.
`(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#aaa accounting default vrf management group radius`	Enable accounting for radius server configured for vrf management
`(config)#aaa accounting default group radius`	Enable accounting for radius server configured for default vrf

Validation

```
#show aaa accounting vrf management
                VRF: management
  default: group radius

#show aaa accounting vrf all
                VRF: management
  default: group radius

                VRF: default
  default: group radius

#show aaa accounting
                VRF: default
  default: group radius
#
#show running-config aaa
aaa authentication login default vrf management group radius
aaa accounting default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management
```

```
aaa authentication login default  group radius
aaa accounting default  group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1
```

Sample Radius Clients.conf File

```
client 10.12.58.20 {
  secret    = testing123
  shortname = localhost
}
client 192.168.1.2 {
  secret    = testing123
  shortname = localhost
}
client 10.12.37.196 {
  secret    = testing123
}
client 100.0.0.2 {
  secret    = testing123
  shortname = localhost
}

# IPv6 Client
#client ::1 {
#       secret          = testing123
#       shortname       = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
```

Sample Radius Users Configuration File

```
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User
```

```
# On no match, the user is denied access.

selftest Cleartext-Password := "password"
testuser1 Cleartext-Password := "user1@101"
testuser2 Cleartext-Password := "user2@202"
testuser3 Cleartext-Password := "user3@303"
```

CHAPTER 11 DHCP Relay Agent Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

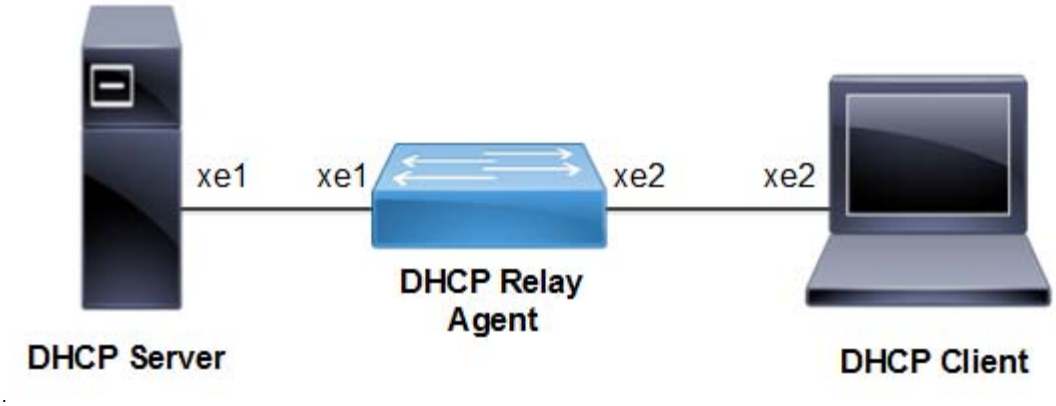


Figure 11-16: DHCP Relay Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)# ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#show running-config dhcp

ip dhcp relay address 10.10.10.2
interface xe2
 ip dhcp relay
!
interface xe1
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Disabled
  DHCP Servers configured: 10.10.10.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe2                      Downlink
  xe1                      Uplink

#show ip dhcp relay address
 VRF Name: default
  DHCP Servers configured: 10.10.10.2
```

DHCP Relay for IPv6 Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#sh ipv6 dhcp relay address

VRF Name: default
  DHCPv6 Servers configured: 2001::2

#show running-config dhcp

Ipv6 dhcp relay address 2001::2
 interface xe2
 ipv6 dhcp relay
!
interface xe1
 ipv6 dhcp relay uplink
!
```

DHCP Relay option 82

This section contains examples of DHCP Relay option-82 configuration. DHCP option 82 (Agent Information Option) provides additional security when DHCP is used to allocate network addresses. It enables the DHCP relay agent to prevent DHCP client requests from untrusted sources. Service Providers use remote identifier (option 82 sub option 2) for troubleshooting, authentication, and accounting. The DHCP Option 82 Remote ID Format feature adds support for the interpretation of **remote-IDs** that are inserted by end users. On the relay agent, you can configure information option to add option 82 information to DHCP requests from the clients before forwarding the requests to the DHCP server. When configured with option 82 and remote-id, the server will receive the DHCP request packet with Agent Circuit ID and remote-id.

The two examples below, show how to configure the DHCP Relay option 82:

- Configuration of DHCP Relay option 82 on a physical interface with Agent information and remote-id.
- Configuration of DHCP Relay option 82 on a VLAN interface with Agent information and remote-id.

Topology

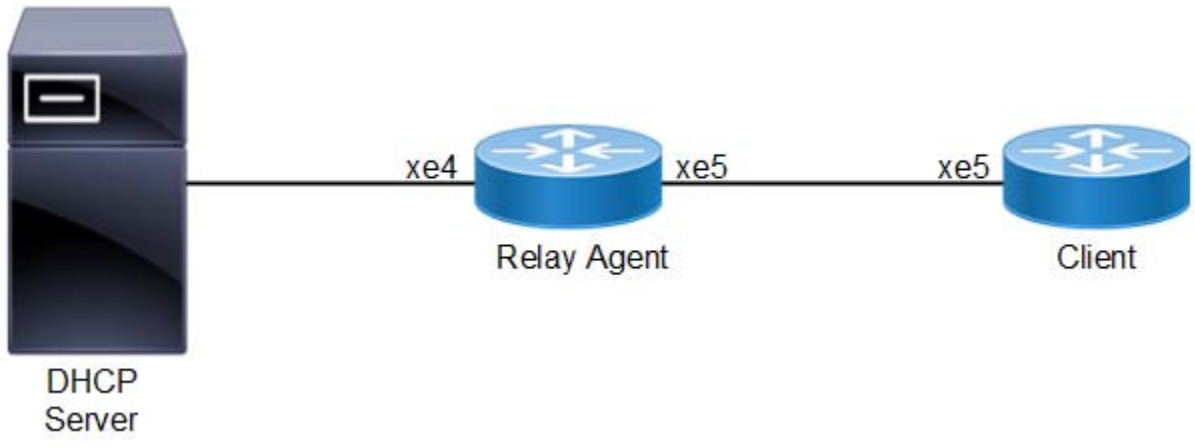


Figure 11-17: DHCP 82 interface topology

Physical Interface Configuration

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent.

Relay agent

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay
(config)#ip dhcp relay address 192.168.1.2	The relay address configured should be server interface address connected to DUT machine
(config)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
(config)#interface xe5	Enter interface mode.
(config-if)#ip address 10.10.20.2/24	Add IP address
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip address 192.168.1.1/24	Configure ipv4 address on the interface xe4
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#exit	Exit interface mode.

Client

#configure terminal	Enter configure mode.
(config)#interface xe5	Enter interface mode.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!

#show ip dhcp relay
```

```
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe5                      Downlink
  xe4                      Uplink
```

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
    Option: (255) End
```

```
        Option End: 255
    Padding
```

Physical Interface Configuration with non-default VRF

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent.

Relay agent

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay.
(config)#ip vrf vrf_dhcp	Configuring non default vrf vrf_dhcp
(config-vrf)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82 on non default vrf.. String support is also provided for remote-id.
(config-vrf)#ip dhcp relay address 192.168.1.2	Configure DHCP relay address in non default vrf.
(config)#interface xe5	Enter interface mode.
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp.
(config-if)#ip address 10.10.20.2/24	Add IP address.
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address.
(config-if)#exit	Exit interface mode.

Client

#configure terminal	Enter configure mode.
(config)#interface xe5	Enter interface mode.
config-if)#ip vrf forwarding vrf_dhcp	Configure ip vrf forwarding for non default vrf.
(config-if)#ip address dhcp	Configure IP address DHCP.
(config-if)#exit	Exit from interface mode.

Validation

Relay Agent

```
#show running-config dhcp
!
ip vrf vrf_dhcp
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf_dhcp
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface               Uplink/Downlink
  ---------               -------------
  xe5                     Downlink
  xe4                     Uplink
```

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
```

```
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
    Option: (255) End
        Option End: 255
    Padding
```

```
Sample DHCP configuration for using Remote-id

class "remote-id" {
        match if option agent.remote-id = OcNOS
} # remote-id

subnet 10.10.20.0 netmask 255.255.255.0 {
        pool {
                allow members of                "remote-id";
                default-lease-time               600;
                max-lease-time                    7200;
                range                           10.10.20.3 10.10.10.100;
                option routers                  10.10.20.2;
                option broadcast-address        10.10.20.255;
                option subnet-mask              255.255.255.0;
                option domain-name-servers      4.2.2.2;
}
```

VLAN Interface Configuration

Topology

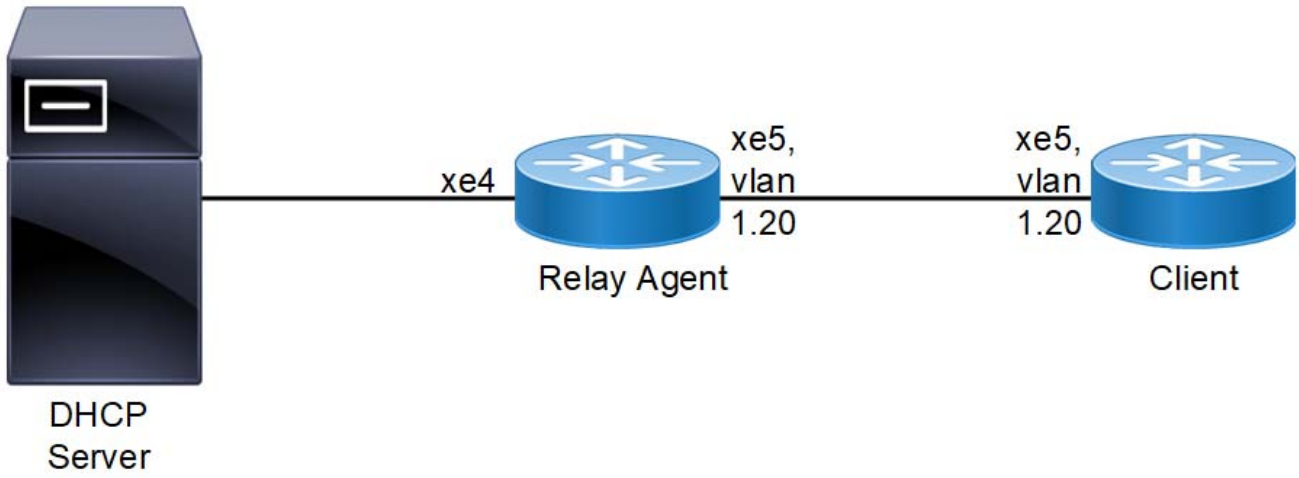


Figure 11-18: DHCP 82 vlan topology

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnets 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent. In the above topology, vlan 20 is part of interface xe5 in relay Agent and xe5 in Client.

Relay Agent

t

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay
`(config)#ip dhcp relay information option remote-id hostname`	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
`(config)#ip dhcp relay address 192.168.1.2`	Configure DHCP relay address
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge
`(config)#vlan 2-100 bridge 1 state enable`	Enable some VLANs
`(config)#interface xe5`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Configure bridge-group
`(config-if)#switchport mode hybrid`	Configure switchport mode
`(config-if)#switchport hybrid allowed vlan all`	Enable vlan
`(config-if)#exit`	Exit from interface mode
`(config)#interface vlan1.20`	Enter interface mode for the vlan interface towards client.
`(config-if)#ip address 10.10.20.2/24`	Add IP address
`(config-if)#ip dhcp relay`	Configure DHCP relay on the vlan interface connecting to client.

(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address
(config-if)#exit	Exit interface mode.

Client

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan 2-100 bridge 1 state enable	Enable VLANs
(config)#interface xe5	Enter interface mode.
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode hybrid	Configure switchport mode
(config-if)#switchport hybrid allowed vlan add 20 egress-tagged enable	Enable vlan
(config-if)#exit	Exit from interface mode
(config)#interface vlan1.20	Enter interface mode for the vlan interface which connects relay.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
!
interface vlan1.20
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!


#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Enabled
  Remote Id: ocnos
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
```

```
  Vlan1.20                Downlink
  xe4                     Uplink
```

Client

```
#show ip interface brief |include vlan1.20
vlan1.20            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x59591459
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 17
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 8
            Agent Circuit ID: 766c616e312e3230
        Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53

   Option: (255) End
        Option End: 255
```

CHAPTER 12 NTP Client Configuration

Overview

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

SNTP is a simplified form of NTP that does not reach the level of accuracy compared to a full implementation of NTP. SNTP can be used for simple applications where the requirements for accuracy and reliability are not too demanding. OcNOS supports SNTP version 4, defined in RFC 2030.

Note: OcNOS uses “`ntp`” for the SNTP command names instead of “`sntp`.”

Support for Default VRF via In-band Management

OcNOS now offers support for NTP over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can either be running on the default or management VRF. By default, it runs on the management VRF.

NTP Modes

The following describes the various NTP node types.

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the others, and each device can also provide time synchronization to the others.

Authentication

For additional security, you can configure your NTP servers and clients to use authentication. Routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the ntp authentication-key vrf management command. A unique number identifies each NTP key. This number is the first argument to the ntp authentication-key vrf management command.
3. 3.Use the ntp trusted-key vrf management command to tell the router which keys are valid for authentication. If a key is trusted, the system will be ready to synchronize to a system that uses this key in its NTP packets. The trusted key should already be configured and authenticated.

NTP Configuration

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server

After configuring the NTP servers, wait a few minutes before you verify that clock synchronization is successful. When the clock synchronization has actually happened, there will be an '*' symbol along with the interface while you give the "`show ntp peers`" command.

Topology

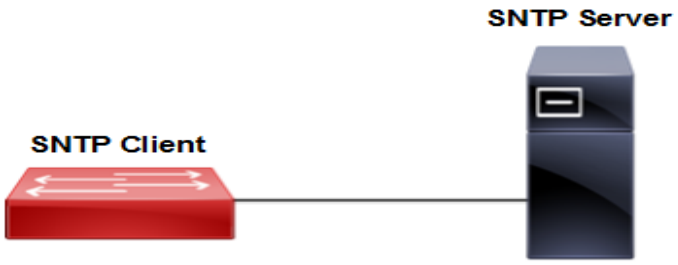


Figure 12-19: SNTP Client and Server

NTP Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)# ntp enable vrf management`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

    #show ntp peer-status
```

```
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the `maxpoll` option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the `minpoll` option.

The client will retry between `minpoll` and `maxpoll` range configured for synchronization with the server.

Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp server 10.1.1.1 maxpoll 7 minpoll 5 vrf management`	Configure `minpoll` and `maxpoll` range for ntp server.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

#show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Enable feature on default or management VRF. By default this feature runs on management VRF..
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#ntp authenticate vrf management`	Enable NTP Authenticate. NTP authentication is disabled by default.
`(config)#ntp authentication-key 1234 md5 text vrf management`	Configure ntp authentication key along with md5 value.
`(config)#ntp trusted-key 1234 vrf management`	Configure trusted key <1-65535>
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp authentication-status
    Authentication enabled

#show ntp authentication-keys
    --------------------------
     Auth Key       MD5 String
    --------------------------
    1234              SWWX

#show ntp trusted-keys
    Trusted Keys:
    1234
```

CHAPTER 13 Simple Network Management Protocol

Overview

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as communities. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption

SNMP is defined in RFCs 3411-3418.

Topology

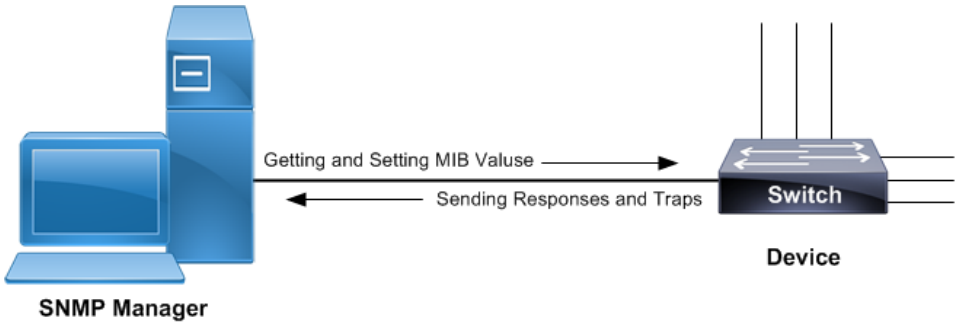


Figure 13-20: SNMP sample topology

Standard SNMP Configurations

`#configure terminal`	Enter configure mode.
`(config)#snmp-server view all .1 included vrf management`	Creates SNMP view labeled as “all” for OID-Tree as “.1” for vrf management.
`(config)#snmp-server community test group network-operator vrf management`	Set community string as “test” for group of users having “network-operator” privilege.
`(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management`	Specify host “10.12.6.63” to receive SNMP version 2 notifications at udp port number 162 with community string as “test”.
`(config)#snmp-server enable snmp vrf management`	Use this command to start the SNMP agent.
`(config)#exit`	Exit configure mode.

Validation

Use the below commands to verify the SNMP configuration:

```
#show running-config snmp
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management

#show snmp group
-------------------------------------------------------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
-------------------------------------------------------------------------------
test          network-operator    2c/1       all        none           all

#show snmp host
-------------------------------------------------------------------------------
Host                Port   Version   Level          Type           SecName
-------------------------------------------------------------------------------
10.12.6.63          162    2c        noauth         trap           test
```

SNMP GET Command

```
# snmpget -v2c -c test 10.12.45.238
.1.3.6.1.2.1.6.13.1.2.10.12.45.238.22.10.12.6.63.52214

TCP-MIB::tcpConnLocalAddress.10.12.45.238.22.10.12.6.63.52214 = IpAddress:
10.12.45.238
```

SNMP WALK Command

SNMP WALK for particular OID

```
#snmpwalk -v2c -c test 10.12.45.238 .1.3.6.1.2.1.25.3.8.1.8
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.1 = STRING: 0-1-1,0:0:0.0
```

```
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.4 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.5 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.6 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.10 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.12 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.13 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.14 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.15 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.16 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.17 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.18 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.19 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.20 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.21 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.22 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.23 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.24 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.25 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.26 = STRING: 0-1-1,0:0:0.0
```

Complete SNMP WALK

```
#snmpwalk -v2c -c test 10.12.45.238 .1
```

SNMP WALK Command

```
#snmpset -v2c -c test 10.12.45.102 1.3.6.1.2.1.10.246.1.2.1.30.1 u 123
iso.3.6.1.2.1.10.246.1.2.1.30.1 = Gauge32: 123
```

CHAPTER 14 Access Control Lists Configurations

This chapter contains a complete example of access control list (ACL) configuration.

Overview

An Access Control List is a list of Access Control Entries (ACE). Each ACE in ACL specifies the access rights allowed or denied.

Each packet that arrives at the device is compared to each ACE in each ACL in the order they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

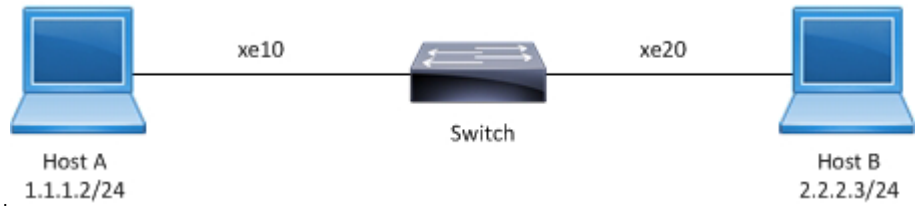


Figure 14-21: ACL sample topology

IPv4 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list T1`	Create an IP access list named T1.
`(config-ip-acl)#deny any host 1.1.1.1 any`	Create an access rule to deny IP packets with source address 1.1.1.1.
`(config-ip-acl)#permit any host 1.1.1.1/24 any`	Create an access rule to permit IP packets with source address 1.1.1.1.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group T1 in`	Apply access group T1 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.1, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists T1
IP access list T1
        10 deny any host 1.1.1.1 any [match=200]
        20 permit any 1.1.1.1/24 any
        default deny-all
```

When inbound IP packets reach interface xe10 with a source address in the range from 1.1.1.1 to 1.1.1.254, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists T1
IP access list T1
    10 deny any host 1.1.1.1 any
    20 permit any 1.1.1.1/24 any [match=2000]
    default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

ICMP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Create an IP access list named icmp-acl-01.
`(config-ip-acl)#10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 fragments`	Create an access rule with sequence number 10 to deny ICMP packets from a specific source towards a specific destination with a DSCP value of af11. Note: The sequence number is optional.
`(configip-acl)#20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash`	Create an access rule with sequence number 20 to permit ICMP packets from a specific source towards a specific destination with precedence as flash.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group icmp-acl-01 in`	Apply access group icmp-acl-01 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.X, destination address 2.2.2.X, DSCP value af11, and are fragmented, then the count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 [match=200]
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
```

```
    default deny-all
```

When inbound IP packets reach interface xe10 with source address as 1.1.1.X, destination address 2.2.2.X, and precedence value flash, then the count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
    default deny-all
```

Note: Use the command `clear ip access-list counters` to clear statistics of all ACLs configured or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

Access List Entry Sequence Numbering

You can change the sequence numbers of rules in an access list.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Enter access list mode for ACL icmp-acl-01.
`(config-ip-acl)#resequence 100 200`	Re-sequence the access list, starting with sequence number 100 and incrementing by 200.
`(config-ip-acl)#1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11`	Re-sequencing specific access rule 100 with sequence number 1000
`(config-ip-acl)#exit`	Exit access list mode.

Validation

Before re-sequencing:

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
        20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
        default deny-all
```

After re-sequencing the access list, starting with sequence number 100 and incrementing by 200

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        100 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
        300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
        default deny-all
```

After re-sequencing specific access rule 100 with sequence number 1000

```
 #show access-lists icmp-acl-01
IP access list icmp-acl-01
300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
default deny-all
```

IPv6 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ipv6 access-list ipv6-acl-01`	Create an IPv6 access list named as icmp-acl-01.
`(config-ipv6-acl)#11 deny ip any any flow-label 100`	Create access rule sequence number 11 to deny IPv4 encapsulated packets in IPv6 with any source address to any destination address with flow label 100.
`(config-ipv6-acl)#default permit-all`	Update the default rule to permit all.
`(config-ipv6-acl)#exit`	Exit access list mode
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ipv6 address 1:1::1:3/64`	Assign an IPv6 address.
`(config-if)#ipv6 access-group ipv6-acl-01 in`	Apply access group ipv6-acl-01 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IPv6 packets reach interface xe10 with IPv4 packets encapsulated with flow label 100, then count for access rule 11 increases equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ip any any flow-label 100 [match=1000]
    default permit all
```

For all other IPv6 packets, access rule 100 is invoked and the match counts increase equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ip any any flow-label 100
    default permit-all [match=2000]
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list <ipv6 access-list name> counters` to clear statistics of the particular IPv6 ACL.

MAC ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#mac access-list mac-acl-01`	Create a MAC access list named mac-acl-01.
`(config-mac-acl)#22 permit host 0000.0011.1212 host 0000.1100.2222 vlan 2`	Create an access rule with sequence number 22 to permit packets from a host with a specific MAC towards a host with a specific MAC with VLAN 2.
`(config-mac-acl)#exit`	Exit access list mode.

`(config)#bridge 1 protocol rstp vlan-bridge`	Create a VLAN-aware RSTP bridge.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2.
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#mac access-group mac-acl-01 in`	Applies the MAC access list mac-acl-01 to ingress traffic.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound packets reach interface xe10 with the specific source and destination MAC with the VLAN as 2, then the count for access rule 22 increases equal to the number of packets sent.

```
#show mac access-lists
MAC access list mac-acl-01
    22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2 [match=3000]
    default deny-all
```

For all other packets, default rule is invoked and the match counts increases equal to the number of packets sent.

```
#show mac access-lists mac-acl-01
MAC access list mac-acl-01
    22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2
    default deny-all [match=2000]
```

Note: As per the present design, ARP/ND packets will be filtered based on the source MAC address only (host mac address).

Note: Use the command `clear mac access-list counters` to clear statistics of all MAC ACLs or `clear mac access-list <mac access-list name> counters` to clear statistics of a particular MAC ACL.

Management ACL Overview

Management Port ACL can be used to provide basic level of security for accessing the management network. ACLs can also be used to decide which types of management traffic to be forwarded or blocked at the management port.

When configuring access list on a router or a switch, each access list needs to be identified by a unique name or a number. Each access list entry can have permit or deny actions. Each entry will be associated with a sequence number in the range of <1-268435453>. Lower the sequence number, higher the priority.

User should be able to configure the system to allow certain IP address for a protocol and don't allow any other IP address matching for that protocol.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

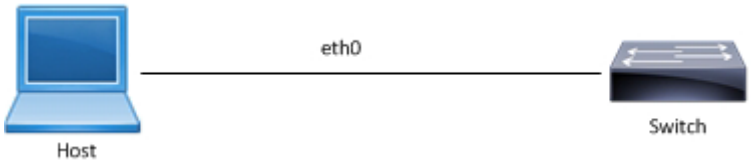


Figure 14-22: Management ACL Sample Topology

Management ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list mgmt`	Create an IP access list named mgmt
`(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh`	Create an access rule to permit TCP connection with source address 10.12.45.57 with destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet`	Create an access rule to permit TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq snmp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to SNMP.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq ntp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to NTP.
`(config-ip-acl)#permit udp host 10.12.29.49 any eq snmptrap`	Create an access rule to permit UDP packet with source address 10.12.29.49 with any Destination address on destination port equal to SNMPTrap.
`(config-ip-acl)#permit tcp host 10.12.29.49 eq ssh host 10.12.45.57`	Create an access rule to permit TCP connection with source address 10.12.29.49 on source port equal to ssh with Destination address 10.12.45.57 .
`(config-ip-acl)#deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh`	Create an access rule to deny TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet`	Create an access rule to deny TCP connection with source address 10.12.45.57 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 10.12.29.49/24`	Assign an IP address.
`(config-if)#ip access-group mgmt in`	Apply access group mgmt for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When a TCP connection for Destination Port SSH reach interface eth0 with source address 10.12.45.57, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection for Destination Port Telnet reach interface eth0 with source address 10.12.45.58, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet [match=10]
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port SNMP reach interface eth0 with any source address, then the match count for access rule 30 increases equal to the number of packets sent. Prior to this SNMP should be configured on Device (10.12.29.49).

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

    #show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp [match=50]
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port NTP reach interface eth0 with any source address, then the match count for access rule 40 increases equal to the number of packets sent. Prior to this NTP should be configured on Device (10.12.29.49).

```
    Example:
    ntp enable vrf management
    ntp authenticate vrf management
    ntp authentication-key 123 md5 swwx 7 vrf management
    ntp trusted-key 123 vrf management
    ntp server 10.12.45.36 vrf management
    ntp server 10.12.16.16 prefer vrf management
```

```
    ntp server 10.12.16.16 key 123 vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp [match=1]
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port SSH reach interface eth0 with source address 10.12.45.58, this should deny the connection and the match count for access rule 70 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh [match=1]
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port Telnet reach interface eth0 with source address 10.12.45.57, this should deny the connection and the match count for access rule 80 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet[match=1]
            default deny-all
```

To enable SNMPTRAPS, apply the ACL outbound to the Management interface.

`#configure terminal`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#ip access-group mgmt out`	Apply access group mgmt for outbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

When a UDP packet for Destination Port SNMPTrap sends out of interface eth0 with any Destination address, then the match count for access rule 50 increases equal to the number of packets received. Prior to this SNMPTrap should be configured on Device (10.12.29.49) to listen to port 162.

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
```

```
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap [match=5]
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When an ACL is applied on interface eth0 outbound and inbound together, then we must configure an ACL to establish a TCP connection between source 10.12.29.49 with source Port SSH to destination address 10.12.45.57. When a TCP connection is established on port SSH, then the match count for access rule 10 and 60 increases equal to the number of packets sent and received.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57[match=9]
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

```
#show access-lists
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet


#show access-lists summary
     IPV4 ACL mgmt
           statistics enabled
           Total ACEs Configured: 8
           Configured on interfaces:
              eth0 - ingress (Router ACL)
           Active on interfaces:
              eth0 - ingress (Router ACL)

#show access-lists expanded
```

```
IP access list mgmt
        10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
        20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
        30 permit udp any host 10.12.29.49 eq snmp
        40 permit udp any host 10.12.29.49 eq ntp
        50 permit udp host 10.12.29.49 any eq snmptrap
        60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
        70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
        80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
        default deny-all [match=4]
```

ARP ACL Overview

ARP ACL can be used to permit or deny the ARP packets, based on the ARP request or response option configured.

Topology

Figure 14-23: ARP ACL Sample Topology

ARP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge4`	m
`(config-if)#ip address`	Assign IPv4 address.
`(config-if)#exit`	Exit access list mode.
`(config)#mac access-list mac1`	Enter mac access list mode.
`(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp request`	Create an access rule to permit specific ARP request.
`(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp response`	Create an access rule to permit specific ARP response.
`(config-mac-acl)#permit any any ipv4`	Create an access rule to permit any IPv4 packet.
`(config-mac-acl)#exit`	Exit access list mode.
`(config)#interface ge4`	Enter interface mode.
`(config-if)#mac access-group mac1 in`	Apply access group mac1 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to assign IP address on IXIA and ping from IXIA.

```
#show mac access-lists
    MAC access list mac1
            10 permit host 0000.3AE0.456D any arp request [match=1]
            20 permit host 0000.3AE0.456D any arp response [match=1]
            30 permit any any ipv4 [match=1]
            default deny-all
```

ACL over Loopback

The loopback interface ACL feature provides basic security for management applications accessible through In-band interfaces.

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

Topology

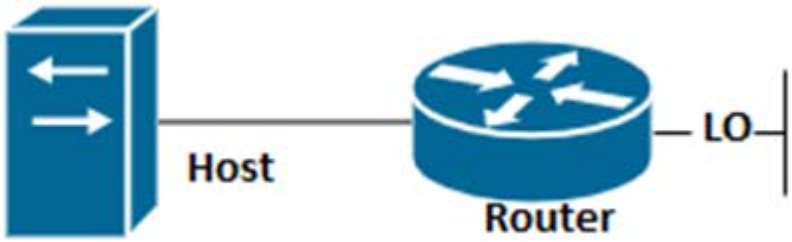


Figure 14-24: ACL Loopback Topology

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 4.4.4.4/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 5.5.5.5/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 6.6.6.6/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 7.7.7.7/32 secondary`	Assign the IPv4 secondary address.
`(config-if)# exit`	Exit interface mode.
`(config)#ip access-list loopback`	Create loopback access list
`(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet`	Permit telnet session from any source with specific destination.
`(config-ip-acl)# 20 deny tcp any host 4.4.4.4 eq telnet`	Deny telnet session from any source with specific destination.
`(config-ip-acl)# 30 permit tcp any host 5.5.5.5 eq ssh`	Permit ssh session from any source with specific destination.
`(config-ip-acl)# 40 deny tcp any host 6.6.6.6 eq ssh`	Deny ssh session from any source with specific destination.
`(config-ip-acl)# 50 deny udp any host 6.6.6.6 eq snmp`	Deny udp from any source with specific destination.

`(config-ip-acl)# 60 deny udp any host 7.7.7.7 eq ntp`	Deny udp from any source with specific destination.
`(config-ip-acl)#exit`	Exit interface acl mode
`(config)#interface lo`	Enter interface lo mode
`(config-if)#ip access-group loopback in`	Associate loopback acl over lo interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

Validation

```
#sh access-lists
IP access list loopback
        10 permit tcp any host 3.3.3.3 eq telnet [match=12]
        20 deny tcp any host 4.4.4.4 eq telnet [match=12]
        30 permit tcp any host 5.5.5.5 eq ssh
        40 deny tcp any host 6.6.6.6 eq ssh
        50 deny udp any host 6.6.6.6 eq snmp  [match=6]
        60 deny udp any host 7.7.7.7 eq ntp

#sh ip access-lists summary
 IPV4 ACL loopback
       statistics enabled
       Total ACEs Configured: 6
       Configured on interfaces:
          lo - ingress (Router ACL)
       Active on interfaces:
          lo - ingress (Router ACL)
       Configured on line vty:

#sh running-config aclmgr
ip access-list loopback
 10 permit tcp any host 3.3.3.3 eq telnet
 20 deny tcp any host 4.4.4.4 eq telnet
 30 permit tcp any host 5.5.5.5 eq ssh
 40 deny tcp any host 6.6.6.6 eq ssh
 50 deny udp any host 6.6.6.6 eq snmp
 60 deny udp any host 7.7.7.7 eq ntp
!
interface lo
 ip access-group loopback in
!
```

ACL over Virtual Terminal

When a Telnet or SSH connection is made, OcNOS associates the connection with a virtual terminal (VTY) line. The ACL over VTY feature provides security for management features associated with VTY.

Standard ACLs are supported on VTY lines. Any standard ACL rule when applied on a VTY line permits/denies only management access ports such as SSH, Telnet, SNMP, and NTP.

Note: IPv6 and "out" filters for standard ACLs on VTY lines are not supported.

This is an example configuration:

```
#show run access-list
ip access-list standard abc
permit host 1.1.1.1
deny any
!

#show ip access-lists summary
 IPV4 STANDARD ACL abc
       Total ACEs Configured: 2
       Configured on interfaces:
       Active on interfaces:
       Configured on line vty:
          all vty lines - ingress
```

Topology

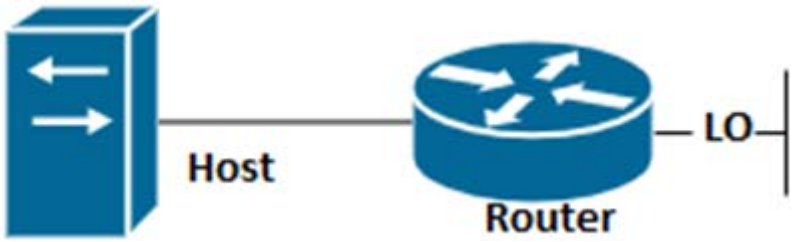


Figure 14-25: Line VTY ACL

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 4.4.4.4/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 5.5.5.5/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 6.6.6.6/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 7.7.7.7/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip access-list vty`	Create loopback access list
`(config-ip-acl)#10 permit tcp any host 3.3.3.3 eq telnet`	Permit telnet session from any source with specific destination.
`(config-ip-acl)#20 deny tcp any host 4.4.4.4 eq telnet`	Deny telnet session from any source with specific destination.
`(config-ip-acl)#30 permit tcp any host 5.5.5.5 eq ssh`	Permit ssh session from any source with specific destination.
`(config-ip-acl)#40 deny tcp any host 6.6.6.6 eq ssh`	Deny ssh session from any source with specific destination.
`(config-ip-acl)#50 deny udp any host 6.6.6.6 eq snmp`	Deny udp from any source with specific destination.
`(config-ip-acl)#60 deny udp any host 7.7.7.7 eq ntp`	Deny udp from any source with specific destination.

(config-ip-acl)#exit	Exit interface acl mode
(config)#line vty	Enter Line vty mode
(config-all-line)#ip access-group vty in	Associate acl over VTY
(config-all-line)#end	Exit interface mode
(config)#exit	Exit config mode

Validation

```
#sh access-lists
IP access list vty
        10 permit tcp any host 3.3.3.3 eq telnet [match=53]
        20 deny tcp any host 4.4.4.4 eq telnet
        30 permit tcp any host 5.5.5.5 eq ssh
        40 deny tcp any host 6.6.6.6 eq ssh [match=4]
        50 deny udp any host 6.6.6.6 eq snmp
        60 deny udp any host 7.7.7.7 eq ntp

#sh ip access-lists summary
 IPV4 ACL vty
       statistics enabled
       Total ACEs Configured: 6
       Configured on interfaces:
       Active on interfaces:
       Configured on line vty:
          all vty lines - ingress

#sh running-config aclmgr

ip access-list vty
 10 permit tcp any host 3.3.3.3 eq telnet
 20 deny tcp any host 4.4.4.4 eq telnet
 30 permit tcp any host 5.5.5.5 eq ssh
 40 deny tcp any host 6.6.6.6 eq ssh
 50 deny udp any host 6.6.6.6 eq snmp
 60 deny udp any host 7.7.7.7 eq ntp
!
line vty
 ip access-group vty in
```

CHAPTER 15 Route-map Continue Configuration

This section contains Route-map continue configuration with BGP.

Overview

The continue clauses allow you to configure and organize more modular policy definitions to reduce the number of policy configurations that are repeated within the same route map.

Continue clause under a route-map provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses. The continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicates the order in which clauses are to be evaluated.

Using Continue with Match Clauses

When a `match` clause exists in a route-map with continue clause then `continue` clause is executed only when a successful match occurs. If a `match` clause does not exist in the route-map and if a `continue` clause exists, the `continue` clause will be evaluated and will go to the specified route-map entry. When a successful match occurs and we have a `continue` clause, the route-map executes the `set` clauses and then goes to the specified route-map entry. If a `continue` clause does not exist in the next route map, then the route-map will behave normally. If a `continue` clause exists in the next route-map but a match is not successful, the route-map will not continue and will “fall through” to the next sequence number if one exists

Using Continue with Set Actions

`Set` clauses are executed after the route-map evaluation is done. The `set` clauses are evaluated and executed in the order in which they were configured. `Set` clauses are only executed after a successful match occurs. The `continue` statement proceeds to the specified route-map entry only after configured `set` actions are performed. If a `set` action is configured in the first route-map and then the same `set` action occurs again but with a different value, in a subsequent route-map entry, then the last `set` action will override the previous `set` actions which were configured with the same set command.

Topology

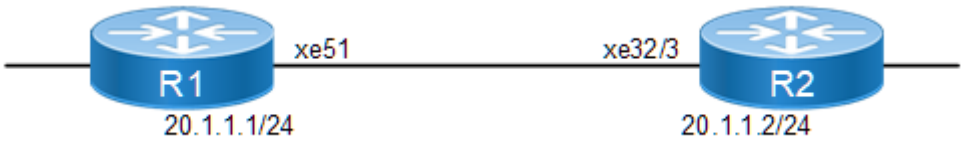


Figure 15-26: Route-map continue

Configure Route-map *continue* on R1

In the below example we will apply route-map `continue` on R1 under BGP 100, with redistributed connected routes from R2 on R1. Here, 10.1.0.0/16 is a superset, while 10.1.1.0/24, 10.1.2.0 /24, 10.1.3.0/24, 10.1.4.0/24, and 10.1.5.0/24 are subsets and will filter PF1, which is a superset and sets several prefixes.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe51`	Enter interface mode.
`R1(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#ip prefix-list PF1 seq 5 permit 10.1.0.0/16 le 32`	Configure super set prefix PF1
`R1(config)#ip prefix-list P1 seq 5 permit 10.1.1.0/24 le 32`	Configure subset prefix P1
`R1(config)#ip prefix-list P2 seq 5 permit 10.1.2.0/24 le 32`	Configure subset prefix P2
`R1(config)#ip prefix-list P3 seq 5 permit 10.1.3.0/24 le 32`	Configure subset prefix P3
`R1(config)#router bgp 100`	Configure bgp process 100
`R1(config-router)#bgp router-id 1.1.1.1`	Configure bgp router id
`R1(config-router)#neighbor 20.1.1.2 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`R1(config-router)#neighbor 20.1.1.2 route-map myid1 in`	Configure bgp route-map myid1 as In bound policy with neighbor ip
`R1(config-routed)#exit`	Exit the router bgp mode
`R1(config)#route-map myid1 permit 1`	Configure route-map myid1 with sequence number 1
`R1(config-route-map)match ip address prefix-list PF1`	Match for prefix PF1
`R1(config-route-map)continue`	Configure continue command without sequence number
`R1(config-route-map)set metric 10`	Set metric as 10
`R1(config-route-map)set weight 3465789`	Set weight as 3465789
`R1(config-route-map)route-map myid1 permit 2`	Configure route-map myid1 with sequence number 2
`R1(config-route-map)match ip address prefix-list P1`	Match for IP prefix-list P1
`R1(config-route-map)continue 3`	Configure continue with sequence number 3
`R1(config-route-map)set metric 20`	Set metric as 20.
`R1(config-route-map)set origin igp`	Set origin as IGP protocol
`R1(config-route-map)route-map myid1 permit 3`	Configure route-map myid1 with sequence number 3
`R1(config-route-map)match ip address prefix-list P2`	Match for IP prefix-list P2
`R1(config-route-map)continue 4`	Configure continue with sequence number 4
`R1(config-route-map)set metric 30`	Set metric as 30.
`R1(config-route-map)set as-path prepend 600`	Set as-path prepend as 600
`R1(config-route-map)route-map myid1 permit 4`	Configure route-map myid1 with sequence number 4
`R1(config-route-map)match ip address prefix-list P3`	Match for IP prefix-list P3.
`R1(config-route-map)set local-preference 400`	Set local preference as 400
`R1(config-route-map)set weight 400`	Set weight as 400
`R1(config-route-map)end`	End the route-map

R2

R2#configure terminal	Enter configure mode.
R2(config)#interface xe32/1	Enter interface mode.
R2(config-if)#ip address 10.1.1.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/2	Enter interface mode.
R2(config-if)#ip address 10.1.2.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/4	Enter interface mode.
R2(config-if)#ip address 10.1.3.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe17/1	Enter interface mode.
R2(config-if)#ip address 10.1.4.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe21/1	Enter interface mode.
R2(config-if)#ip address 10.1.5.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/3	Enter interface mode.
R2(config-if)#ip address 20.1.1.2/24	Configure the IP address on the connected interface.
R2(config-if)#exit	Exit interface mode.
R2(config)#router bgp 100	Configure BGP process 100
R2(config-router)#bgp router-id 2.2.2.2	Configure BGP router id
R2(config-router)#neighbor 20.1.1.1 remote-as 100	Configure BGP remote-as 100 with neighbor IP
R2(config-router)#redistribute connected	Redistribute the connected routes which are 10 networks here.

Validation

R1

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 5
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
20.1.1.2                 4   100  145        177       5      0      0
00:40:05              5

Total number of neighbors 1

Total number of Established sessions 1

Note: Check the prefixes learnt here are 5.
```

```
R1#

R1#show ip bgp
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  10.1.1.0/24      20.1.1.2              20        100           3465789  i
*>i  10.1.2.0/24      20.1.1.2              30        100           3465789 600
?
*>i  10.1.3.0/24      20.1.1.2              10        400           400      ?
*>i  10.1.4.0/24      20.1.1.2              10        100           3465789  ?
*>i  10.1.5.0/24      20.1.1.2              10        100           3465789  ?

Total number of prefixes 5
R1#
```

Note: In the above example, 10.1.4.0/24 and 10.1.5.0/24 prefixes will match only on PF1 which is a super set prefix and metric is set as 10, while the 10.1.1.0/24, 10.1.2.0/24 and 10.1.3.0/24 prefixes will match in P1, P2 and P3 prefix-lists and execute the set clauses respectively.

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     10.1.1.0/24 [200/20] via 20.1.1.2, xe51, 00:45:05
B     10.1.2.0/24 [200/30] via 20.1.1.2, xe51, 00:45:05
B     10.1.3.0/24 [200/10] via 20.1.1.2, xe51, 00:45:05
B     10.1.4.0/24 [200/10] via 20.1.1.2, xe51, 00:25:05
B     10.1.5.0/24 [200/10] via 20.1.1.2, xe51, 00:24:35
C     20.1.1.0/24 is directly connected, xe51, 01:00:40
C     127.0.0.0/8 is directly connected, lo, 02:26:41

Gateway of last resort is not set
R1#

R1#show ip bgp route-map myid1
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  10.1.1.0/24      20.1.1.2              20        100           3465789  i
```

```
*>i  10.1.2.0/24      20.1.1.2              30        100           3465789 600
?
*>i  10.1.3.0/24      20.1.1.2              10        400           400      ?
*>i  10.1.4.0/24      20.1.1.2              10        100           3465789  ?
*>i  10.1.5.0/24      20.1.1.2              10        100           3465789  ?

Total number of prefixes 5
R1#
R1#
```

R2

```
R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
20.1.1.1                 4   100  133        133       3      0      0
00:39:57              0

Total number of neighbors 1

Total number of Established sessions 1
R2#
R2#


R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   10.1.1.0/24      0.0.0.0              0         100           32768    ?
*>   10.1.2.0/24      0.0.0.0              0         100           32768    ?
*>   10.1.3.0/24      0.0.0.0              0         100           32768    ?
*>   10.1.4.0/24      0.0.0.0              0         100           32768    ?
*>   10.1.5.0/24      0.0.0.0              0         100           32768    ?
*>   20.1.1.0/24      0.0.0.0              0         100           32768    ?

Total number of prefixes 6
R2#

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default
```

```
    IP Route Table for VRF "default"
    C     10.1.1.0/24 is directly connected, xe32/1, 01:02:22
    C     10.1.2.0/24 is directly connected, xe32/2, 01:01:46
    C     10.1.3.0/24 is directly connected, xe32/4, 01:02:21
    C     10.1.4.0/24 is directly connected, xe17/1, 00:26:52
    C     10.1.5.0/24 is directly connected, xe21/1, 00:26:32
    C     20.1.1.0/24 is directly connected, xe32/3, 01:02:22
    C     127.0.0.0/8 is directly connected, lo, 01:34:40

    Gateway of last resort is not set
    R2#
```

Route-map Show Commands

```
R1#show running-config route-map
    !
    route-map myid1 permit 1
     match ip address prefix-list PF1
     continue
     set metric 10
     set weight 3465789
    !
    route-map myid1 permit 2
     match ip address prefix-list P1
     continue 3
     set metric 20
     set origin igp
    !
    route-map myid1 permit 3
     match ip address prefix-list P2
     continue 4
     set metric 30
     set as-path prepend 600
    !
    route-map myid1 permit 4
     match ip address prefix-list P3
     set local-preference 400
     set weight 400
    !
    R1#
R1#show route-map
    route-map myid1, permit, sequence 1
      Match clauses:
        ip address prefix-list: PF1
      Continue clause:  next sequence
      Set clauses:
        metric 10
        weight 3465789
    route-map myid1, permit, sequence 2
      Match clauses:
        ip address prefix-list: P1
      Continue clause:  sequence 3:
      Set clauses:
        metric 20
```

```
    origin igp
route-map myid1, permit, sequence 3
  Match clauses:
    ip address prefix-list: P2
  Continue clause:  sequence 4:
  Set clauses:
    metric 30
    as-path prepend 600
route-map myid1, permit, sequence 4
  Match clauses:
    ip address prefix-list: P3
  Set clauses:
    local-preference 400
    weight 400
```

CHAPTER 16 Show Tech Support Configurations

Overview

OcNOS maintains a collection of consolidated information about system configurations and statistics. This information is for debugging and diagnosing system issues.

Note: Output is displayed on the terminal.

Tech Support Samples

`#show tech-support`	Collects system configurations and statistics for all modules.

CHAPTER 17 Debounce Timer

The debounce timer avoids frequent updates (churn) to higher layer protocols during flapping of an interface. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to minimum of 1.5 times the value of the debounce time. Otherwise it could affect the protocol states if the debounce timer is still running.

Topology

Figure 17-27 is a simple deployment using the debounce timer

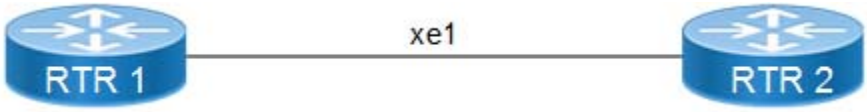


Figure 17-27: Debounce timer

RTR 1

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)#debounce-time 4000`	Configure debounce-time as 4000ms
`(config)#exit`	Exit configure mode

RTR 2

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)#debounce-time 4000`	Configure debounce-time as 4000ms
`(config)#exit`	Exit configure mode.

Validation

```
#show running-config
debounce-time 4000
#show interface xe1
Debounce timer: enabled
Debounce-time 4000 ms
Flap Count: 0
Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1
Debounce timer: enabled
Debounce-time 4000 ms
Flap Count: 1
Last Debounce Flap : 2019 Aug 14 17:24:33 (00:00:10 ago)
Debounce status : idle

#show interface xe1
Debounce timer: enabled
Debounce-time 4000 ms
Flap Count: 1
Last Debounce Flap : 2019 Aug 14 17:24:35 (00:00:16 ago)
Debounce status : idle
```

Log Messages

The following is a configuration example to log debounce timer activity:

`#configure terminal`	Enter Configure mode
`(config)#logging level nsm 7`	Enable operational log to display debounce start and end.

Example Log Messages

```
2019 Aug 14 17:24:32.532 : rtr1 : NSM : INFO : Start Debounce Timer on interface xe1, prev_state UP new_state DOWN
2019 Aug 14 17:24:33.810 : rtr1 : NSM : INFO : Interface xe1 Flapped, prev_state UP new_state UP,flap count 1
2019 Aug 14 17:24:36.532 : rtr1 : NSM : INFO : Debounce Timer Expired on interface xe1, prev_state UP, new_state UP
```

System Management Command Reference

Contents

This document contains these chapters and appendices:

CHAPTER 1 Dynamic Host Configuration Protocol Client

This chapter describes the Dynamic Host Configuration Protocol (DHCP) client commands.

DHCP is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

This chapter contains these commands:

feature dhcp

Use this command to enable the DHCP client and DHCP relay on the device.

Use the no form of this command to disable the DHCP client and DHCP relay and delete any DHCP-related configuration.

Command Syntax

```
feature dhcp
no feature dhcp
```

Parameters

None

Default

By default, feature dhcp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature dhcp
```

ip address dhcp

Use this command to get an IP address from a DHCP server for this interface.

Use the no form of this command to disable the DHCP client for this interface.

You can give the ip dhcp client request command before giving this command to request additional options.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip address dhcp
(config-if)#
```

ip dhcp client request

Use this command to add an option to a DHCP request.

Use the no form of this command to remove an option from a DHCP request.

Command Syntax

```
ip dhcp client request dns-nameserver
ip dhcp client request host-name
ip dhcp client request log-server
ip dhcp client request ntp-server
no ip dhcp client request dns-nameserver
no ip dhcp client request host-name
no ip dhcp client request log-server
no ip dhcp client request ntp-server
```

Parameters

`dns-nameserver`	List of DNS name servers (DHCP option 6)
`host-name`	Name of the client (DHCP option 12)
`ntp-server`	List of NTP servers (DHCP option 42)
`log-server`	List of log servers (DHCP option 7)

Default

By default, ip dhcp client request is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip dhcp client request ntp-server
```

CHAPTER 2 Domain Name System

This chapter describes Domain Name System (DNS) commands. DNS translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol (IP).

Note: The commands below are supported only on the “management” VRF.

The chapter contains these commands:

debug dns client

Use this command to display DNS debugging messages.

Use the no form of this command to stop displaying DNS debugging messages.

Command Syntax

```
debug dns client
no debug dns client
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dns client
```

ip domain-list

Use this command to define a list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.

The `ip domain-list` command is similar to the ip domain-name command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If there is no domain list, the default domain name specified with the `ip domain-name` command is used. If there is a domain list, the default domain name is not used.

Use the `no` form of this command to remove a domain.

Command Syntax

```
ip domain-list (vrf management|) DOMAIN-NAME
no ip domain-list (vrf management|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain name, such as company.com

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-list mySite.com
```

ip domain-lookup

Use this command to enable DNS host name-to-address translation.

Use the no form of this command to disable DNS.

Command Syntax

```
ip domain-lookup (vrf management|)
no ip domain-lookup (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-lookup
```

ip domain-name

Use this command to set the default domain name used to complete unqualified host names (names without a dotted-decimal domain name).

The ip domain-list command is similar to the `ip domain-name` command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If a domain list has been created with ip domain-list, the default domain name is not used. If there is no domain list, the default domain name is used.

Use the `no` form of this command to disable DNS.

Command Syntax

```
ip domain-name (vrf management|) DOMAIN-NAME
no ip domain-name (vrf management|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain name, such as company.com

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-name company.com
```

ip host

Use this command to define static hostname-to-address mappings in DNS. You can specify one or two mappings in a command.

Use the no form of this command remove a hostname-to-address mapping.

Command Syntax

```
ip host (vrf management|) WORD A.B.C.D
ip host (vrf management|) WORD A.B.C.D A.B.C.D
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD A.B.C.D
no ip host (vrf management|) WORD A.B.C.D A.B.C.D
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`WORD`	Host name, such as company.com
`X:X::X:X`	IPv6 address of the host
`A.B.C.D`	IPv4 address of the host

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip host company.com 192.0.2.1
```

ip name-server

Use this command to add 1-3 DNS server addresses that are used to translate hostnames to IP addresses.

Use the no form of this command to remove 1-3 DNS server addresses.

Command Syntax

```
ip name-server (vrf management|) A.B.C.D
ip name-server (vrf management|)(A.B.C.D) (A.B.C.D)
ip name-server (vrf management|) (A.B.C.D) (A.B.C.D) (A.B.C.D)
ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
  (X:X::X:X | A.B.C.D)
no ip name-server (vrf management|) A.B.C.D
no ip name-server (vrf management|) A.B.C.D A.B.C.D
no ip name-server (vrf management|) A.B.C.D A.B.C.D A.B.C.D
no ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
no ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
no ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
  (X:X::X:X | A.B.C.D)
```

Parameters

management	Virtual Routing and Forwarding name
A.B.C.D	IPv4 address of the host
X:X::X:X	IPv6 address of the host

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip name-server 123.70.0.23
```

show hosts

Use this command to display the DNS name servers and domain names.

Command Syntax

```
show hosts (vrf management|all)
```

Parameters

`vrf`	management or all VRFs

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying two name servers: 10.10.0.2 and 10.10.0.88.

```
#show hosts
       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 2-2 explains the output fields.

Table 2-2: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF.
DNS lookup is enabled	DNS feature enabled or disabled.
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 2-2: show hosts fields

Entry	Description
Host	Static hostname-to-address mappings in DNS.
Test	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	Name-server indicates it has been learned dynamically.

show running-config dns

Use this command to show the DNS settings of the running configuration.

Command Syntax

```
show running-config dns (vrf management|)
```

Parameters

vrf	management

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config dns
ip domain-lookup vrf management
ip domain-name vrf management .com
ip domain-list vrf management .in
ip domain-list vrf management .ac
ip name-server vrf management 10.12.3.23
ip host vrf management test 10.12.12.67 10::23
```

CHAPTER 3 Secure Shell

This chapter describes Secure Shell (SSH) commands.

SSH is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

clear ssh hosts

Use this command to clear the `known_hosts` file.

This command clears all trusted relationships established with SSH servers during previous connections. When a client downloads a file from an external server the first time, the client stores the server keys in the `known_hosts` file. After that, other connections to the same server will use the server keys stored in the `known_hosts` file. In other words, a trusted relationship is created when a client accepts the server keys the first time.

An example of when you need to clear a trusted relationship is when SSH server keys are changed.

Command Syntax

```
clear ssh hosts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ssh hosts
```

debug ssh server

Use this command to display SSH server debugging information.

Use the no form of this command to stop displaying SSH server debugging information.

Command Syntax

```
debug ssh server
no debug ssh server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ssh server
```

feature ssh

Use this command to enable the SSH server.

Use the no form of this command to disable the SSH server.

Command Syntax

```
feature ssh (vrf management|)
no feature ssh (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature ssh
```

show debug ssh-server

Use this command to display whether SSH debugging is enabled.

Command Syntax

```
show debug ssh-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug ssh-server
ssh server debugging is on
```

show running-config ssh server

Use this command to display SSH settings in the running configuration.

Command Syntax

```
show running-config ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config ssh server
feature ssh vrf management
ssh server port 1024 vrf management
ssh login-attempts 2 vrf management
ssh server algorithm encryption 3des-cbc
```

show ssh key

Use this command to display the SSH server key.

By default, ssh feature is enabled in "management" vrf. Until and unless the same feature is explicitly enabled in "default" vrf, respective show command output will be empty.

Command Syntax

```
show ssh key vrf management
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ssh key
******************RSA KEY*********************
 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj

 bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48

************************************
******************DSA KEY*********************
 ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=

 bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52

************************************
```

show ssh server

Use this command to display the SSH server status.

Command Syntax

```
show ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ssh server
ssh server enabled port: 22
authentication-retries 3
```

show username

Use this command to display the RSA or DSA key pair for a user.

Command Syntax

```
show username USERNAME keypair
```

Parameters

USERNAME	User identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show username OcNOS keypair
***************RSA KEY*******************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCnWo/3Y7LlVkw/Z43dbVIm+I3o25JlgUTmwa9ll
T35+2gNvDbIPfYAqUKYgrmXKDc9vg7f4SAsmXS+4ZwrrQSTTsHk8PNLA+4lEcufFNl3jpfXTuhphN9
N9
i+uFHGYIIviWZksiRqpMZmDlALyzAIOzyCfG44hlRm3/
pYfhBNhHruvxYVhbP4wHsmrWfcFb+HZCWQGM
CJupxu8bouGd2UW5/BlVy1yuYNIhdo2NHjUI+ameETV+Wroki8+OLVA6eXp5/
KY3Bj9x2+AxOCiKcpU0
axwFSoCbP3+29wrp4JJhl4ssSqM+19+VbUtpuXAM0cR7VQ7mJ0JDZ9tBvK4l8/
bitcount: 2048 fingerprint: 2b:ac:17:a4:ef:1d:79:4e:2d:17:af:72:4c:c7:e4:2f
***********************************
***************DSA KEY*******************
ssh-dss AAAAB3NzaC1kc3MAAACBAP0npAm+Pw8t7OpO+KQ0Vx3ayXavHHVPPAKOo8RTmquE8zUSjn
/XiZ+vP2343RpXu9/
jLwAcCUMfNBZyE8NbmGKxMMk2PqMz10VtfvDOn5LSNurXL4lypZLG2hR2PNva4w
6b4Adpd+E1fEoUncIgOun2i4SO8N5TCMYVyusKjYzDAAAAFQCWeAzeahZeoIzBlnSo87madxfL3QAA
AI
EA4b86l/
nHoWobRoYBrkeOGtjyWLRKk1P2T+rGH+j0rqqJiD0sh2PVfppylliNvqLtYSmXyMCxzEEeFd
HH1cVXgrgQjtUOeCPhF+2We2ummmlCwg4v71Z358FRjsi9VgJ/vQUpOq1hRDhwjJHtEHSA+NkX/
ccW9J
ww8YOoNhCI7DcAAACANuYiP6tKGSU9LeClF1F65Tq1blVHfLp3TSeZYPldqonDoZ1qo3NNvOOH5KN8
Lj
MRtTCN1GaXow1QccS941XFy3efuWXxC00HZ64FhmjCyOYYv2Wsvn4UGCAG3ikiu6M1xjOLl6b53H4m
B3
w7O6bkcjH1GnytwrgR0D/nlsZ/9fs=
bitcount: 1024 fingerprint: c1:0a:e5:e1:a1:78:ae:c2:4a:07:4a:50:07:4b:d5:84
***********************************
```

ssh

Use this command to open an ssh session to a ipv4 address or host name resolved to an ipv4 address.

Command Syntax

```
ssh WORD (vrf (NAME | management))
ssh WORD <1-65535> (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc| aes256-cbc | 3des-cbc)) WORD  (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc | aes256-cbc | 3des-cbc)) WORD <1-65535> (vrf (NAME | management))
```

Parameters

WORD	User and Destination Host name to resolve into IPV4 Address or IPv4 Address to open a ssh session as user@ipv4-address/Hostname
1-65535	Destination Port to open a ssh session. Default is 22
cipher	Specify algorithm to encrypt ssh session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, ssh WORD option is 22

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh cipher aes128-ctr 10.12.16.17 22 vrf management
The authenticity of host '10.12.16.17 (10.12.16.17)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
Are you sure you want to continue connecting (yes/no)?
```

ssh6

Use this command to open an ssh session to an ipv6 address or host name resolved to an ipv6 address.

Command Syntax

```
ssh6 (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
  aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
  aes256-cbc | 3des-cbc))  (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME |
  management))
```

Parameters

X:XX::X:X	User and Destination IPv6 Address to open a ssh session as user@ipv6-address
HOSTNAME	User and Destination Host name to resolve into IPv6 Address to open an ssh session as user@ipv4-address/Hostname
1-65535	Destination Port to open a ssh session. Default is 22
cipher	Specify algorithm to encrypt ssh session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

No default value is specified.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh6 cipher aes128-ctr 2:2::2:2 22 vrf management
The authenticity of host '2:2::2:2 (2:2::2:2)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
```

```
        Are you sure you want to continue connecting (yes/no)?
```

ssh algorithm encryption

SSH server authorizes connection of only those algorithms that are configured from the list below. If a client tries establishing a connection to the server with the algorithm encryption that are not part of the list, the connection will not established.

SSH server supports the encryption algorithms Advanced Encryption Standard Counter Mode [AES-CTR], Advanced Encryption Standard Cipher Block Chaining [AES-CBC], and Triple Data Encryption Standard [3DES].

and they are as follows:

1. aes128-ctr
2. aes192-ctr
3. aes256-ctr
4. aes128-cbc
5. 3des-cbc
6. aes192-cbc
7. aes256-cbc

Use this command to set an algorithm encryption to establish ssh session.

Use the no form of this command to remove an algorithm encryption.

Command Syntax:

```
ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc
  |aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
no ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-
  cbc |aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
```

Parameters

aes18-ctr	AES 128 bit Counter Mode
aes192-ctr	AES 192 bit Counter Mode
aes256-ctr	AES 256 bit Counter Mode
aes128-cbc	AES 128 bit Cipher block chaining
aes192-cbc	AES 192 bit Cipher block chaining
aes256-cbc	AES 256 bit Cipher block chaining
3des-cbc	Triple DES Cipher block chaining
vrf	Virtual Routing and Forwarding
NAME	Virtual Routing and Forwarding name

Default

No default value is specified.

By default, all the ciphers are supported for a new ssh client to connect to the ssh server.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh server algorithm encryption aes128-ctr
```

Note: After configuring the ssh server algorithm encryption, if you disable the previous encryption algorithm, the command is rejected, and the following message is displayed:

```
"% There must be at least one session encryption alogirthm."
```

ssh key

Use this command to create a SSH server key.

Use the no form of this command remove a SSH server key. The `no ssh key` form (with no other parameters) deletes both RSA and DSA keys.

Command Syntax

```
ssh key dsa (vrf management|)
ssh key dsa force (vrf management|)
ssh key rsa (vrf management|)
ssh key rsa length <1024-4096> (vrf management|)
ssh key rsa length <1024-4096> force (vrf management|)
ssh key rsa force (vrf management|)
no ssh key (vrf management|)
no ssh key dsa (vrf management|)
no ssh key rsa (vrf management|)
```

Parameters

`dsa`	Digital System Algorithm (DSA) SSH key
`management`	Virtual Routing and Forwarding name
`force`	Forces the replacement of an SSH key
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 768 bits and the default length is 2048.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh key dsa vrf management
```

ssh login-attempts

Use this command to set the number of times that a user can try to log in to a SSH session.

Use the no form of this command to set the number of login attempts to its default (3).

Command Syntax

```
ssh login-attempts RETRIES (vrf management|)
no ssh login-attempts (vrf management|)
```

Parameters

RETRIES	Number of retries <1-3>
management	Virtual Routing and Forwarding name

Default

By default, the device attempts to negotiate a connection with the connecting host three times.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh login-attempts 3
```

ssh server port

Use this command to set the port number on which the SSH server listens for connections. The default port on which the SSH server listens is 22.

Use the no form of this command to set the default port number (22).

Command Syntax

```
ssh server port <1024-65535> (vrf management|)
no ssh server port (vrf management|)
```

Parameters

<1024-65535>	Port number
management	Virtual Routing and Forwarding name

Default

By default, SSH server port is 22.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh server port 1720
```

username sshkey

Use this command to add public key of the ssh clients to perform pasword-less login into the switch.

Command Syntax

```
username USERNAME sshkey LINE
```

Parameters

USERNAME	User identifier
LINE	Digital System Algorithm (DSA) key or Rivest, Shamir, and Adelman (RSA) key in OpenSSH format; this key is written to the `authorized_keys` file

Default

By default, SSHKEY is 1024.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#username fred
(config)#username fred sshkey
AAAAB3NzaC1kc3MAAAEBAIirweZzCdyITqbMWB8Wly9ivGxY1JBVnWTVtcWKi6uc
CPZyw3I6J6/+69LEkPUSAyO+SK8zj0NF2f25FFc2YDMh1KKHi5gK7iXF3/ran54j
nP2byyLeo8rnuVqfEDLaBI1qQaWBcDQvsZc14t5SEJfsOQSfR03PDqPYAisrZRvM
5pWfzo486Rh33J3+17OuARQtZFDP4wA5zZoFxhl4U3RK42JzKNUiYBDrH3lSgfkv
XLWLXz9WcxY6zuKvXFwUpOA9PRXwUsKQqWuyywZQLNavENqFyoQ8oZnNKLCYE0h8
QnUe62NGxb3jQXKLflOL04JFNiii9sACG1Y/ut4ANysAAAAVAJbM7Z4chRgiVahN
iwXFJNkBmWGZAAABAAuF1FlI6xy0L/pBaIlFw34uUL/mh4SR2Di2X52eK70VNj+m
y5eQdRC6cxpaVqpS3Q4xTN+W/kaBbIlX40xJP5lcjMvfn/nqiuIeEodmVIJMWxOD
fh3egeGuSW614Vzd1RGrxpYInIOygMULRcxhmbX+rPliuUIvhg36iH0UR7XBln6h
uyKFvEmaL7bGlRvELjqaj0y6iiCfP1yGBc5vavH5X+jOWqdsJHsCgcIzPF5D1Ybp
w0nZmGsqO+P55mjMuj0O2uI7Ns1sxyirbnGhd+ZZ1u03QDy6MBcUspai8U5CIe6X
WqvXY+yJjpuvlW9GTHowCcGd6Z/e9IC6VE/kNEAAAAEAFIe6kLGTALR0F3AfapYY
/M+bvkmkkhOJUZVdLiwMjcvtJb9fQpPxqXElS3ZvUNIEElUPS/V7KgSsj8eg3FKN
iUGICkTwHIK7RTLC8k4IE6U3V3866JtxW+Znv1DB7uwnbZgoIZuVt3r1+h8O0ah8
UKwDUMJT0fwu9cuuS3G8Ss/gKi1HgByrcxXoK51/r4Bc4QmR2VQ8sXOREv/SHJeY
JGbEX3OxjRgXC7GlpbrdPiL8zs0dPiZ0ovAswsBOYlKYhd7JvfCcvWRjgP5h55aw
GNSmNs3STKufbIqYGeDAISYNYY4F2JzR593KIBnWgyhokyYybyEBh8NwTTO4J5rT
ZA==
```

username keypair

Use this command to generate the key for users.

Command Syntax

```
username USERNAME keypair rsa
username USERNAME keypair dsa
username USERNAME keypair rsa length <1024-4096>
username USERNAME keypair rsa length <1024-4096> force
username USERNAME keypair rsa force
username USERNAME keypair dsa force
```

Parameters

`USERNAME`	User identifier
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`dsa`	Digital System Algorithm (DSA) SSH key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)
`force`	Forces the replacement of an SSH key

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 1024 bits and the default length is 4096.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#username fred keypair rsa
```

CHAPTER 4 Simple Network Management Protocol

This chapter is a reference for Simple Network Management Protocol (SNMP) commands.

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption.

SNMP is defined in RFCs 3411-3418.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- snmp-server host
- snmp-server location
- snmp-server tcp-session
- snmp-server user
- snmp-server view

clear snmp hostconfig

Use this command to remove all SNMP trap hosts.

Command Syntax

```
clear snmp hostconfig
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear snmp hostconfig
```

debug snmp-server

Use this command to display SNMP debugging information.

Use the no form of this command to stop displaying SNMP debugging information.

Command Syntax

```
debug snmp-server
no debug snmp-server
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug snmp-server
```

show running-config snmp

Use this command to display the SNMP running configuration.

Command Syntax

```
show running-config snmp
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config snmp
snmp-server view all .1 included
snmp-server community abc group network-admin
snmp-server enable snmp
```

show snmp

Use this command to display the SNMP configuration, including session status, system contact, system location, statistics, communities, and users.

Command Syntax

```
show snmp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp
SNMP Protocol:Enabled
sys Contact:
sys Location:

--------------------------------------------------------------------------------
Community Group/Access Context acl_filter
--------------------------------------------------------------------------------
public network-admin
_______________________________________________________________________________

                         SNMP USERS
_______________________________________________________________________________
User Auth Priv(enforce) Groups
_______________________________________________________________________________

SNMP Tcp-session :Disabled
```

show snmp community

Use this command to display SNMP communities.

Command Syntax

```
show snmp community
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp community

-------------------------------------------------------------------------------
-------------------------
Community                    Group/Access        view-name
version
-------------------------------------------------------------------------------
-------------------------
test                                  network-operator
testing                     network-operator          ipi
2c
```

Table 4-3 explains the output fields.

Table 4-3: show snmp community fields

Entry	Description
Community	SNMP Community string.
Group/Access	Community group name.
View-name	Community view name.
Version	Community version.

show snmp engine-id

Use this command to display the SNMP engine identifier.

The SNMP engine identifier is a unique string used to identify the device for administration purposes. You do not specify an engine identifier for a device; OcNOS generates a default string. For more about the SNMP engine identifier, see RFC 2571.

Command Syntax

```
show snmp engine-id
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp engine-id
SNMP ENGINE-ID : 80 00 8f 41 03 00 00 00 00 00 00
```

Table 4-4 explains the output fields.

Table 4-4: show snmp engine-ip fields

Entry	Description
SNMP ENGINE-ID : 80 00 8f 41 03 00 00 00 00 00 00	The SNMP engine identifier is a unique string used to identify the device for administration purposes.

show snmp group

Use this command to display SNMP server groups and associated views.

Command Syntax

```
show snmp group
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp group
--------------------------------------------------------------------------------
-------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
--------------------------------------------------------------------------------
-------------------------------

test          network-operator    2c/1      all          all          all
kedar         network-operator    3         all          none         all
tamil         network-operator    3         all          none         all
```

Table 4-5 explains the output fields.

Table 4-5: show snmp group output

Entry	Description
Community/User	Displays the access type of the user for which the notification is generated.
Group	The name of the SNMP group, or collection of users that have a common access policy.
Version	SNMP version number.
Read-View	A string identifying the read view of the group. For further information on the SNMP views, use the show snmp view command.
Write-View	A string identifying the write view of the group.
Notify-View	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the snmp-server group group-name version notify notify-view command.

show snmp host

Use this command to display the SNMP trap hosts.

Command Syntax

```
show snmp host
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp host
-------------------------------------------------------------------------
Host           Port   Version   Level      Type     SecName
-------------------------------------------------------------------------

10.10.26.123   162    2c        noauth     trap     test
```

Table 4-6 explains the output fields.

Table 4-6: Show snmp host output

Entry	Description
Host	The IP address of the SNMP host server.
Port	The port being used for SNMP traffic.
Version	SNMP version number.
Level	The security level being used.
Type	The type of SNMP object being sent.
SecName	Secure Name for this SNMP session.

show snmp user

Use this command to display SNMP users and associated authentication, encryption, and group.

Command Syntax

```
show snmp user
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp user

SNMP USERS
_____________________________________________________________________
User            Auth    Priv(enforce)     Groups
_____________________________________________________________________
ntwadmin        MD5     AES               network-admin

#
```

Table 4-7 explains the output fields.

Table 4-7: Show snmp user output

Entry	Description
User	The person attempting to use the SMNMP agent.
Auth	The secure encryption scheme being used.
Priv(enforce)	What enforcement privilege is being used (in this case, it is the Advance Encryption Standard).
Group	The group to which the user belongs.

show snmp view

Use this command to display SNMP views.

Command Syntax

```
show snmp view
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp view

View : all
  OID : .1
  View-type : included
```

snmp-server community

Use this command to create an SNMP community string and access privileges.

Use the no form of this command to remove an SNMP community string.

Command Syntax

```
snmp-server community WORD (| (view VIEW-NAME version (v1 | v2c ) ( ro | rw)) |
  (group WORD) |( ro | rw) | (use-acl WORD) ) (vrf management|)
no snmp-server community COMMUNITY-NAME (vrf management|)
```

Parameters

WORD	SNMP community string; maximum length 32 characters
VIEW-NAME	Defined view that defines the objects available to the SNMP community
v1	SNMP v1
v2c	SNMP v2c
ro	Read-only access
rw	Read-write access
group	Community group
WORD	Community group name; maximum length 32 characters
ro	Read-only access
rw	Read-write access
use-acl	Access control list (ACL) to filter SNMP requests
WORD	ACL name; maximum length 32 characters
management	Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server community MyComm view MyView1 version v2c rw vrf
management
```

snmp-server contact

Use this command to set the system contact information for the device (`sysContact` object).

Use the no form of this command to remove the system contact information.

Command Syntax

```
snmp-server contact (vrf management|) (TEXT|)
no snmp-server contact (vrf management|) (TEXT|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`TEXT`	System contact information; maximum length 32 characters without spaces

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server contact vrf management Irving@555-0150
```

snmp-server enable snmp

Use this command to start the SNMP agent daemon over UDP.

Use the no form of this command to stop the SNMP agent daemon over UDP.

Command Syntax

```
snmp-server enable snmp  (vrf management|)
no snmp-server enable snmp  (vrf management|)
```

Parameters

management	Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server enable snmp vrf management
```

snmp-server enable traps

Use this command to enable or disable SNMP traps and inform requests.

Command Syntax

```
snmp-server enable traps (link(linkDown|linkUp|)|snmp(authentication|)|) (vrf
  management|)
no snmp-server enable traps ((link(linkDown|linkUp|))|(snmp(authentication|))|)
  (vrf management|)
```

Parameters

`link`	Module notifications enable
`linkDown`	IETF Link state down notification
`linkUp`	IETF Link state up notification
`snmp`	Enable RFC 1157 notifications
`authentication`	Send SNMP authentication failure notifications
`management`	Virtual Routing and Forwarding name

Default

By default, SNMP server traps are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server enable traps vrf management
```

snmp-server host

Use this command to configure an SNMP trap host. An SNMP trap host is usually a network management station (NMS) or an SNMP manager.

Use the no form of this command to remove an SNMP trap host.

Command Syntax

IPv4/SNMP v2:

```
snmp-server host (A.B.C.D|HOSTNAME) (traps | informs)
  version ((1 | v2c) WORD)  (|udp-port <1-65535>) (vrf management|)
```

IPv4/SNMP v3:

```
snmp-server host (A.B.C.D|HOSTNAME) (traps | informs)
  version(( (1 | 2c) WORD | (3 (noauth | auth | priv) WORD)) (|udp-port <1-65535>)
  (vrf management|)
```

Parameters

A.B.C.D	IPv4 address
HOSTNAME	DNS host name
traps	Send notifications as traps
informs	Send notifications as informs
version	Version
v1	SNMP v1
1	SNMP v1
v2c	SNMP v2c
2c	SNMP v2c
WORD	SNMP community string
<1-65535>	Host UDP port number; the default is 162
management	Virtual Routing and Forwarding name
3	SNMP v3 security level
noauth	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
auth	Authentication and no privacy (authNoPriv) security model: use message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
priv	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
WORD	SNMPv3 user name

Default

The default SNMP version is v2c and the default UDP port is 162.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server host 10.10.10.10 traps version 3 auth MyUser udp-port 512
vrf management
```

snmp-server location

Use this command to set the physical location information of the device (`sysLocation` object).

Use the `no` form of this command to remove the system location information.

Command Syntax

```
snmp-server location (vrf management|) (LINE|)
no snmp-server location (vrf management|) (LINE|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`LINE`	Physical location information

Default

No system location string is set.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server location vrf management Bldg. 5, 3rd floor, northeast
```

snmp-server tcp-session

Use this command to start the SNMP agent daemon over TCP.

Use the no form of this command to close the SNMP agent daemon over TCP.

Command Syntax

```
snmp-server tcp-session (vrf management|)
no snmp-server tcp-session (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, snmp server tcp session is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server tcp-session vrf management
```

snmp-server user

Use this command to create an SNMP server user.

Use the no form of this command to remove an SNMP server user.

Command Syntax

```
snmp-server user WORD (|WORD) ((auth (md5 | sha ) AUTH-PASSWORD) ((priv (des | aes)
  PRIV-PASSWORD) |) |) (vrf management|)
no snmp-server user USER-NAME (vrf management|)
```

Parameters

WORD	User name; length 5-32 characters
WORD	Name of the group to which the user belongs; maximum length 35 characters
auth	Packet authentication type
md5	Message Digest Algorithm 5 (MD5)
sha	Secure Hash Algorithm (SHA)
AUTH-PASSWORD	Authentication password; length 8-32 characters
priv	Packet encryption type (“privacy”)
des	Data Encryption Standard (DES)
aes	Advanced Encryption Standard (AES)
PRIV-PASSWORD	Encryption password; length 8-33 characters
management	Virtual Routing and Forwarding name

Default

By default, snmp server user word is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server user Fred auth md5 J@u-b;l2e`n,9p_ priv des
t41VVb99i8He{Jt vrf management
```

snmp-server view

Use this command to create or update a view entry

Use the no from of this command to remove a view entry.

Command Syntax

```
snmp-server view VIEW-NAME OID-TREE (included | excluded) (vrf management|)
no snmp-server view VIEW-NAME (vrf management|)
```

Parameters

`VIEW-NAME`	View name; maximum length 32 characters
`OID-TREE`	Object identifier of a subtree to include or exclude from the view; specify a text string consisting of numbers and periods, such as 1.3.6.2.4
`included`	Include `OID-TREE` in the SNMP view
`excluded`	Exclude `OID-TREE` from the SNMP view
`management`	Virtual Routing and Forwarding name

Default

By default, snmp-server view VIEW-NAME OID-TREE is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example creates a view named `myView3` that excludes the `snmpCommunityMIB` object (1.3.6.1.6.3.18).

```
#configure terminal
(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded vrf management
```

CHAPTER 5 Telnet

This chapter describes telnet commands.

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

debug telnet server

Use this command to display telnet debugging information.

Use the no form of this command to stop displaying telnet debugging information.

Command Syntax

```
debug telnet server
no debug telnet server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server

telnet server debugging is on
#
```

feature telnet

Use this command to enable the telnet server.

Use the no form of this command to disable the telnet server.

Note: Executing no form command closes the active telnet session.

Command Syntax

```
feature telnet (vrf management|)
no feature telnet (vrf management|)
```

Parameters

management	Virtual Routing and Forwarding name

Default

By default, feature telnet is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature telnet vrf management
```

show debug telnet-server

Use this command to display whether telnet debugging is enabled.

Command Syntax

```
show debug telnet-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server
telnet server debugging is on
```

show running-config telnet server

Use this command to display telnet settings in the running configuration.

Command Syntax

```
show running-config telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config telnet server

telnet server port 1025 vrf management
feature telnet vrf management
```

show telnet-server

Use this command to display the telnet server status.

Command Syntax

```
show telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show telnet server
telnet server enabled port: 23
```

telnet

Use this command to open a telnet session to an ipv4 address or host name resolved to ipv4 address.

Command Syntax

```
telnet (A.B.C.D | HOSTNAME) (vrf (NAME|management))
telnet (A.B.C.D | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

A.B.C.D	Destination IPv4 Address to open a telnet session.
HOSTNAME	Destination Hostname to resolve into IPv4 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet 10.12.16.17 2543 vrf management
Trying 10.12.16.17...
```

telnet6

Use this command to open a telnet session to an ipv6 address or host name resolved to ipv6 address.

Command Syntax

```
telnet6 (X:X::X:X| HOSTNAME) (vrf (NAME|management))
telnet6 (X:X::X:X | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

X:X::X:X	Destination IPv6 Address to open a telnet session.
HOSTNAME	Destination Host name to resolve into IPv6 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet6 2:2::2:2 2543 vrf management
 Trying 2:2::2:2...
```

telnet server port

Use this command to set the port number on which the telnet server listens for connections. The default port on which the telnet server listens is 23.

You can only give this command when the telnet server is disabled. See the feature telnet command.

Use the no form of this command to set the default port number (23).

Command Syntax

```
telnet server (port <1024-65535>) (vrf management|)
no telnet server port (vrf management|)
```

Parameters

`<1024-65535>`	Port number
`management`	Virtual Routing and Forwarding name

Default

By default, telnet server port number is 23

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#telnet server port 1157 vrf management
```

CHAPTER 6 Syslog

This chapter is a reference for the `syslog` commands.

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, an application such as `mail` and `cron` generates messages with a facility names “mail” and “cron”.
- Eight degrees of severity (numbered 0-7) of the message which are explained in Table 6-8.

This chapter contains these commands:

Syslog Severitie

Note: The prefixes of the example logs are all removed. i.e. Following full log "2020 Apr 12 11:20:27.612 : 17U-18U : PSERV : MERG : !!! hsl Module crashed, System reboot halted as it rebooted continuosly 2 times" is captured as "hsl Module crashed,System reboot halted as it rebooted continuosly 2 times".

Table 6-8: Syslog severities (Sheet 1 of 2)

Severity Level	Keyword	Description

0	emergency	The whole system is unusable and needs operator intervention to recover. If only a particular port or component is unusable, but the system as a whole is still usable it is not categorized at an emergency level.
		Examples of this type of message:
		`Output Power of PSU XX (psu_no) XX Watt] has exceeded Maximum Output Power Limit[XX Watt]`
		`OSPF Initialization failed.`

1	alert	The operator needs to act immediately or the system might go into emergency state. The system or one of its component's functionality might be critically affected.
		Examples of this type of message:
		`Temperature of sensor is (curr_temp)C. It is nearing Emergency Condition.`
		`OSPF has exceed lsdb limit`
		`OSPF Detected router with duplicate router ID [ID]`

2	critical	A critical system event happened which requires the operator's attention. The event might not require immediate action, but this event can affect functionality or behavior of a system component.
		Examples of this type of message:
		`OSPF Neighbor session went down.`
		`Interface %s changed state to down`

3	error	An error event happened which does not require immediate attention. This log message provides details about error conditions in the system or its components which you can use to troubleshoot problems.
		These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as `debug ospf all`).
		Examples of this type of message:
		`Device i2c bus open error.!!!`
		`[DECODE] Attr ASPATH: Invalid AS Path value.`
		`OSPF MD5 authentication error`

4	notification	Notifications about important system and protocol events to assure the operator that the system is running properly. If a critical/alert condition has happened and has been corrected, that is also logged at this level.
		Examples of this type of message:
		`OSPF Received link up for interface: xe1`
		`OSPF neighbour [10.1.1.1] Status change Exstart -> Exchange`
		`Interface %s changed state to UP`

Table 6-8: Syslog severities (Sheet 2 of 2)

Severity Level	Keyword	Description

5	informational	Detailed informational events happening across the system and protocol modules. These events are not necessarily important and are useful only to find details about the functionality being executed in the system and its components. Some of these events might be periodic events like hello or keep alive messages along with packet dumps. Also, this level includes logs for control packets that are ignored and do not impact the protocol states.
		IP Infusion Inc. recommends to use proper debug filters to log only relevant events and switch off other events; otherwise the logs can get verbose. For example:
		`debug ospf all`
		`no debug ospf packet hello`
		The above enables all OSPF debugging, but disables the periodic hello messages.
		Examples of this type of message:
		`Successfully added dynamic neighbour`
		`[DECODE] KAlive: Received!`
		`[FSM] Ignoring Unsupported event <EVENT> in state <STATE>`
		`Unknown ICMP packet type"`
		`OSPF RECV[%s]: From %r via %s: Version number mismatch`
		`OSPF RECV[%s]: From %r via %s: Network address mismatch`

6	debug informational	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.
7	debug detailed	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.

Log File Rotation

Log rotation is important to maintain the stability of the device, because the larger log files are difficult to manipulate and file system would run out of space. The solution to this common problem is Log File Rotation.

Log rotation is scheduled to happen for every 5 minutes, here the log file size is used as the condition to perform rotation.

Log rotate operation creates a backup of the current log file, and clears the current log file content. Also these rotated log files are compressed to save disk space. Excluding the current log file, four backup files are maintained in the system, and the older logs are removed as part of the rotation operation.

Default log file `/var/log/messages` rotated, if the size is greater than 100 MB. The following are the rotated log files generated in the path `/var/log`

```
root@OcNOS:/var/log# ls messages*
messages  messages.1  messages.2.gz  messages.3.gz  messages.4.gz
```

Manually configured log file `/log/LOG1` gets rotated, if its size is greater than configured size. Here `LOG1` is the manually configured using the command `logging logfile <filename>` and the log file size in bytes can be configured using the command `logging logfile LOG1 <severity> size <4096-419430400>`

```
OcNOS(config)#logging logfile LOG1 7 size 4096
```

Here configured logging file `/log/LOG1` is rotated if the size is greater than 4096 bytes. The following are the rotated log files generated in the path `/log`

```
root@OcNOS:/log# ls LOG*
LOG1  LOG1.1  LOG1.2.gz  LOG1.3.gz  LOG1.4.gz
```

clear logging logfile

Use this command to clear the existing contents of the configured logging logfile.

Note: If the name of the configured logging log file is “mylogfile”, this command clears only the log file mylogfile. But the other rotated or compressed log files are untouched.

Command Syntax

```
clear logging logfile
```

Parameters

None

Default

No default value is specified

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS-SP version 3.0.

Example

```
#clear logging logfile
```

feature rsyslog

Use this command to enable the rsyslog server.

Use the no form of this command to disable the rsyslog server.

Command Syntax

```
feature rsyslog vrf (management|)
no feauture rsyslog vrf (management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature rsyslog vrf management
```

debug logging

Use this command to display logging debugging information.

Use the no form of this command stop displaying logging debugging information.

Command Syntax

```
debug logging host
no debug logging host
```

Parameters

None

Command Mode

Exec and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug logging host
```

log syslog

Use this command to begin logging to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

Command Syntax

```
log syslog
no log syslog
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
```

logging console

Use this command to set the severity level that a message must reach before the messages is sent to the console. The severity levels are from 0 to 7 as shown in Table 6-8.

Use the no form of this command to disable logging console messages.

Note: Below message will be displayed if console severity is set to 6 or 7:

% Warning : If debug volume is huge it can degrade system performance and makes console to be non-responsive

Command Syntax

```
logging console (<0-7>|)
no logging console
```

Parameters

<0-7>	Maximum logging level for console messages as shown in Table 6-8.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 2 (Critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging console 6

(config)#2015 Dec 23 03:13:26 OcNOS BGP-6: [RIB] Scanning BGP Network Route
s...
2015 Dec 23 03:13:41 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:13:56 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:00 OcNOS BGP-6: [RIB] Scanning BGP RIB...
2015 Dec 23 03:14:11 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:26 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:41 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:56 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:15:00 OcNOS BGP-6: [RIB] Scanning BGP RIB...

(config)#no logging console
```

logging level

Use this command to set the severity level that a message for a specific process must reach before the messages is logged. The severity levels are from 0 to 7 as shown in Table 6-8. Logging happens for the messages less than or equal to the configured severity level.

Use the no form of this command to disable logging messages.

Note: Default log level is 2 to report Emergency-0, Alert-1 and Critical-2 level events.

Command Syntax

```
logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|onm|oam|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp) <0-7>
no logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|oam|onm|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp)
```

Parameters

`all`	All messages
`auth`	Auth messages
`bgp`	BGP messages
`dvmrp`	DVMRP messages
`hostp`	Hostp messages
`hsl`	HSL messages
`isis`	ISIS messages
`l2mrib`	L2MRIB messages
`lacp`	LACP messages
`lagd`	LAGD messages
`ldp`	LDP messages
`mrib`	MRIB messages
`mstp`	MSTP messages
`ndd`	NDD messages
`nsm`	NSM messages
`oam`	OAM messages
`onm`	ONM messages
`ospf`	OSPF messages
`ospf6`	OSPF6 messages
`pim`	PIM messages
`pon`	PON messages
`pservd`	PSERVD messages
`ptp`	PTP messages
`rib`	RIB messages

`rip`	RIP messages
`ripng`	RIPNG messages
`rmon`	RMON messages
`rsvp`	RSVP messages
`sflow`	Sflow messages
`vrrp`	VRRP messages
`<0-7>`	Severity level as shown in Table 6-8.

Default

By default, the logging level is 2 (critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging level all 5

#configure terminal
(config)#logging level bgp 6

(config)#no logging monitor
```

logging logfile

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing debug output and command history to the disk file in the directory `/log/`.

When logging logfile is enabled, OcNOS log information is stored in user configured logging file which is present in "/log" directory. The log is spread across four files total of these files size is the user configured size.

For example, if the name of the logging log file is “mylogFile” and logging file size configured is 4 MB then each file will be maximum size of 1MB. The logging file names will be "mylogFile", "mylogfile.0", "mylogfile.1" and "mylogfile.2".

"mylogFile" will have the latest log information. As soon as it’s size becomes 1 MB this file is renamed as mylogFile.0 and newlog information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost in order to accommodate new set of logs in mylogFile.

Use option no to cancel writing to a specific log file.

Note: Changing logfile paramenters (name/size/severity) will be taken into effect for the next OcNOS session.

Command Syntax

```
logging logfile LOGFILENAME <0-7> ((size <4096-4194304>)|)
no logging logfile
```

Parameter

`LOGFILENAME`	Name of the log file.
`<0-7>`	Severity level as shown in Table 6-8.
`<4096-4194304>`	Log file size in bytes.

Default

By default, log file size is 4194304 bytes.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
#configure terminal
(config)#logging logfile test123 7
```

logging monitor

Use this command to set the severity level that a message must reach before a monitor message is logged. The severity levels are shown in Table 6-8.

Use the no parameter to disable logging monitor messages.

Command Syntax

```
logging monitor (<0-7>|)
no logging monitor
```

Parameters

<0-7>	Maximum logging level for monitor messages as shown in Table 6-8.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 3 (error).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging monitor 6

(config)#no logging monitor
```

logging server

Use this command to set a syslog server.

OcNOS supports logging messages to a syslog server in addition to logging to a file or the console (local or ssh/telnet console). OcNOS messages can be logged to a local syslog server (the machine on which OcNOS executes) as well as to one or more remote syslog servers.

Use the `no` form of this command to remove a syslog server.

Note: Only one facility is supported for all protocol modules across all the configured logging servers.

Command Syntax

```
logging server (A.B.C.D|HOSTNAME) (|((<0-7>) (|facility (local0| local1 | local2 |
  local3| local4 |local5 | local6 | local7 |user)))) (vrf management|)
no logging server (A.B.C.D | HOSTNAME ) (vrf management|)
```

Parameters

`A.B.C.D`	IPv4 address
`HOSTNAME`	Host name; specify `localhost` to log locally
`<0-7>`	Severity at which messages are logged as shown in Table 6-8. If not specified, the default is 3.
`facility`	Entity logging the message (user defined); if not specified, the default is local7
`local0`	Local0 entity
`local1`	Local1 entity
`local2`	Local2 entity
`local3`	Local3 entity
`local4`	Local4 entity
`local5`	Local5 entity
`local6`	Local6 entity
`local7`	Local7 entity (default)
`user`	User entity
`management`	Virtual Routing and Forwarding name

Default

If not specified, the default severity at which messages are logged is 3 (error).

If not specified, the default `facility` is `local7`.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging server MyLogHost vrf management

(config)#no feature rsyslog vrf management
(config)#
(config)#feature rsyslog
(config)#logging server 10.10.10.10 7
```

Note: In the latter configuration, the default VRF does not need not to be specified in the command.

logging timestamp

Use this command to set the logging timestamp granularity.

Use the no form of this command to reset the logging timestamp granularity to its default (milliseconds).

Note: Any change in timestamp configurations will result in timestamp configured for event logged by protocol modules except for CLI history for the current and active sessions. The timestamp configuration is reflected in CLI history for new CLI sessions.

Changing logging timestamp will be taken into effect for the next OcNOS session.

Command Syntax

```
logging timestamp (microseconds|milliseconds|seconds|none)
no logging timestamp
```

Parameters

`microseconds`	Microseconds granularity
`milliseconds`	Milliseconds granularity
`seconds`	Seconds granularity
`none`	no timestamp in log message

Default

By default, logging time stamp granularity is milliseconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging timestamp milliseconds
```

show logging

Use this command to display the logging configuration.

Command Syntax

```
show logging (info|level|server|console|timestamp|monitor)
```

Parameters

`info`	Show server logging configuration
`level`	Show facility logging configuration
`server`	Syslog server configuration
`console`	Console configuration
`timestamp`	Timestamp configuration
`monitor`	Monitor configuration

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging console
Console logging     : enabled Severity: Operator (critical) Level : 2


#show logging monitor
Logging monitor     : enabled Severity: Operator (debugging) Level: 7


#show logging server
  Remote Servers:
               1.1.1.1
               severity: Operator (informational)
               facility: local7
               VRF : management

#sh logging info
  Remote Servers:
               1.1.1.1
               severity: Operator (informational)
               facility: local7
               VRF : management
Logging console     : enabled Severity: operator (critical) Level : 2
Logging monitor     : enabled Severity: Operator (debugging) Level : 7
Logging timestamp   : seconds
File logging        : enabled  File Name   : /log/abc  Severity   : Operator (de
```

```
bugging)  Level   : 7  Size   : 4194304
Cli logging         : enabled

Facility        Default Severity        Current Session Severity
nsm                     2                       2
ripd                    2                       2
ripngd                  2                       2
ospfd                   2                       2
ospf6d                  2                       2
isisd                   2                       2
hostpd                  2                       2
mribd                   2                       2
pimd                    2                       2
authd                   2                       2
mstpd                   2                       2
onmd                    2                       2
HSL                     2                       2
oamd                    2                       2
vlogd                   2                       2
vrrpd                   2                       2
ndd                     2                       2
ribd                    2                       2
bgpd                    2                       2
l2mribd                 2                       2
hslrasmgr               2                       2
lagd                    2                       2
pservd                  2                       2
cmmd                    2                       2
```

show logging last

Use this command to display lines from the end of the log file.

Command Syntax

```
show logging last (<1-9999>)
```

Parameters

<1-9999>	Number of lines to display from end of the log file

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging last 100
2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
Connection refused
```

show logging logfile

Use this command to display whether logging is enabled, the log file name, and the logging severity.

Command Syntax

```
show logging logfile
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile
File logging        : enabled  File Name   : /log/abc  Severity   : (7)
2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
logging server 1.1.1.1 5 vrf management '

2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
ex'

2017 Sep 25 17:18:17 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:19:15 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console '

2017 Sep 25 17:19:20 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging monitor '

2017 Sep 25 17:19:32 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging logfile '

2017 Sep 25 17:19:44 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging server '

2017 Sep 25 17:28:26 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:29:02 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console
```

show logging logfile last-index

Use this command to display the number of line in the log file.

Command Syntax

```
show logging logfile last-index
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile last-index
logfile last-index : 10
```

Table 6-9 explains the output fields.

Table 6-9: show logging logfile last-index fields

Entry	Description
logfile last-index	Number of line in the logfile.

show logging logfile start-seqn end-seqn

Use this command to display a range of lines in the log file.

Command Syntax

```
show logging logfile start-seqn (<0-2147483647>) (|(end-seqn <0-2147483647>))
```

Parameters

`start-seqn`	Starting line number
`end-seqn`	Ending line number

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile start-seqn 2 end-seqn 7
2
3 2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile
4
5 2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
6
7 2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
NE4-router#
```

Table 6-10 explains the output fields.

Table 6-10: show logging logfile start-seqn end-seqn fields

Entry	Description
start-seqn	Starting line number
end-seqn	Ending line number

show logging logfile start-time end-time

Use this command to display lines from the log file within a given date-time range.

Command Syntax

```
show logging logfile start-time (<2000-2030> WORD <1-31> WORD) (|(end-time <2000-
  2030> WORD <1-31> WORD))
```

Parameters

start-time	Starting date and time:
<2000-2030>	Year in YYYY format
WORD	Month as jan, feb, mar,..., oct, nov, or dec (maximum length 3 characters)
<1-31>	Day of month in DD format
WORD	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>
end-time	Ending date and time:
<2000-2030>	Year in YYYY format
WORD	Month as jan, feb, mar,..., oct, nov, or dec (maximum length 3 characters)
<1-31>	Day of month in DD format
WORD	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile start-time 2019 Jan 04 06:20:49 end-time 2019 Jan 04
06:21:16
2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile

2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index

2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
#
```

show running-config logging

Use this command to display the logging configuration.

Command Syntax

```
show running-config logging
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config logging
no Logging console
no Logging monitor
logging timestamp milliseconds
```

CHAPTER 7 User Management

This chapter is a reference for user management commands.

This chapter includes these commands:

clear aaa local user lockout username

Use this command to unlock the locked user due to three times wrong password login attempt.

Command Syntax

```
clear aaa local user lockout username USERNAME
```

Parameters

USERNAME	User name; length 2-15 characters

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear aaa local user lockout username testuser
```

clear line

Use this command to clear or close the already opened vty line sessions.

Command Syntax

```
clear line WORD
```

Parameters

```
WORD Enter the Location name (Max Size 64)
```

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User              Idle        Location/Session  PID
TYPE   Role
   (*) 130 vty 0    [C]ocnos              0d00h00m     pts/0
16725   Local  network-admin
#clear line pts/0
Connection closed by foreign host.
-bash-4.1#
```

clear user

Use this command to clear or close the already opened sessions based on the username.

Note: This command will close active telnet sessions if the account being cleared is already active, however the SSH sessions will continue to persist until disconnect.

Command Syntax

clear user WORD

Parameters

`WORD Enter the username (Max Size 28)`

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User              Idle        Location/Session  PID
TYPE   Role
   (*) 130 vty 0    [C]ocnos              0d00h00m     pts/0
16725   Local  network-admin
#clear user ocnos
Connection closed by foreign host.
-bash-4.1#
```

debug user-mgmt

Use this command to display user management debugging information.

Use the no form of this command stop displaying user management debugging information.

Command Syntax

```
debug user-mgmt
no debug user-mgmt
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug user-mgmt

#config t
(config)#debug user-mgmt
```

show user-account

Use this command to display information about all users or a given user.

Command Syntax

```
show user-account (WORD|)
```

Parameters

WORD	User name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show user-account
User:user1
                roles: network-operator
User:user2
                roles: network-operator
User:user3
                roles: network-operator
```

username

Use this command to add a user or to change a user password.

The `role` parameter maps to privilege levels in the TACACS+ server as shown in Table 7-11

Table 7-11: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or greater then 15

Note: You cannot change the `role` parameter for the currently active user.

Use the `no` form of this command to remove a user.

Command Syntax

```
username USERNAME
username USERNAME password (encrypted|) PASSWORD
username USERNAME role (network-admin|network-engineer|network-operator|network-user)
username USERNAME role (network-admin|network-engineer|network-operator|network-user) password (encrypted|) PASSWORD
no username USERNAME
```

Parameters

`USERNAME`	User name; length 2-15 characters
`encrypted`	Password is encrypted
`PASSWORD`	Password; length 5-32 characters
`network-admin`	Network administrator role with all access permissions that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch. Only network administrators can manage other users with the enable password, Authentication, Authorization and Accounting, RADIUS, and TACACS+ commands.
`network-engineer`	Network engineer role with all access permission that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.
`network-operator`	Network operator role with all access permissions that can make temporary changes to the configuration. Changes do not persist after a reset/reboot of the switch.
`network-user`	Network user role with access permissions to display the configuration, but cannot change the configuration.

Default

By default, user name is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#username fred_smith password encrypted W3g7y&6yV}JH6&5EYIah?779IT9iV2
```

CHAPTER 8 Network Time Protocol

This chapter is a reference for Network Time Protocol (NTP) commands.

NTP synchronizes clocks between computer systems over packet-switched networks. NTP can synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

NTP uses a hierarchical, layered system of time sources. Each level of this hierarchy is called a “stratum” and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

clear ntp statistics

Use this command to reset NTP statistics.

Command Syntax

```
clear ntp statistics (all-peers | io | local | memory)
```

Parameters

`all-peers`	Counters associated with all peers
`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ntp statistics all-peers
```

debug ntp

Use this command to display NTP debugging messages.

Use the no form of this command to stop displaying NTP debugging messages.

Command Syntax

```
debug ntp
no debug ntp
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ntp

(config)#no debug ntp
```

feature ntp

Use this command to enable NTP.

Use the no form of this command to disable NTP.

Command Syntax

```
feature ntp (vrf management|)
no feature ntp (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, feature ntp is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature ntp vrf management

(config)#no feature ntp vrf management
```

ntp authenticate

Use this command to enable NTP authentication.

Use the no form of this command to disable authentication.

Command Syntax

```
ntp authenticate (vrf management|)
no ntp authenticate (vrf management|)
```

Parameters

management	Virtual Routing and Forwarding name

Default

By default, ntp authenticate is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp authenticate vrf management
```

ntp authentication-key

Use this command to set an NTP Message Digest Algorithm 5 (MD5) authentication key.

Use the no form of this command to delete an authentication key.

Command Syntax

```
ntp authentication-key <1-65534> md5 WORD (vrf management|)
ntp authentication-key <1-65534> md5 WORD 7 (vrf management|)
no ntp authentication-key <1-65534> md5 WORD (vrf management|)
```

Parameters

`<1-65534>`	Authentication key number
`WORD`	MD5 string (maximum 8 characters)
`7`	Encrypt using weak algorithm
`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp authentication-key 535 md5 J@u-b;l2 vrf management
```

ntp enable

Use this command to enable NTP.

Use the no form of this command to disable NTP.

Command Syntax

```
ntp enable (vrf management|)
no ntp enable (vrf management|)
```

Parameters

management	Virtual Routing and Forwarding name

Default

By default, ntp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp enable vrf management
```

ntp logging

Use this command to log NTP events.

Use the no form of this command to disable NTP logging.

Command Syntax

```
ntp logging (vrf management|)
no ntp logging (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, ntp logging message is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp logging vrf management
```

ntp peer

Use this command to configure a peer association. In a peer association, this system can synchronize with the other system or the other system can synchronize with this system.

Use the no command to remove a peer association.

Command Syntax

```
ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
```

Parameters

A.B.C.D	IPv4 address of peer
HOSTNAME	Host name of peer
X:X::X:X	IPv6 address of peer
prefer	Prefer this peer; preferred peer responses are discarded only if they vary dramatically from other time sources
key	Peer authentication key
<1-65534>	Peer authentication key value
minpoll	Minimum poll interval
<4-16>	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
maxpoll	Maximum poll interval
<4-16>	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
management	Virtual Routing and Forwarding name

Default

By default, value of minpoll is 4 and maxpoll is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ntp peer 10.10.0.23 vrf management
(config)#ntp peer 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp peer 10.10.0.23 vrf management
```

ntp server

Use this command to configure an NTP server so that this system synchronizes with the server, but not vice versa.

Use the no option with this command to remove an NTP server.

Command Syntax

```
ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
no ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
```

Parameters

A.B.C.D	IPv4 address of the server
HOSTNAME	Host name of the server
X:X::X:X	IPv6 address of the server
prefer	Prefer this server; preferred server responses are discarded only if they vary dramatically from other time sources
key	Server authentication key
<1-65534>	Server authentication key
minpoll	Minimum poll interval
<4-16>	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
maxpoll	Maximum poll interval
<4-16>	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
management	Virtual Routing and Forwarding name

Default

By default, minpoll is 4 and maxpoll is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ntp server 10.10.0.23 vrf management
(config)#ntp server 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp server 10.10.0.23 vrf management
```

ntp source-interface

Use this command to configure an NTP source-interface. NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packet are sent.

Use the `no` option with this command to remove an NTP server.

Command Syntax

```
ntp source-interface  IFNAME
```

Parameter

`IFNAME`	Interface name

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced in a version before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ntp source-interface xe7/1
(config)#no ntp source-interface xe7/1
```

ntp sync-retry

Use this command to retry NTP synchronization with configured servers.

Command Syntax

```
ntp sync-retry (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#ntp sync-retry vrf management
```

ntp trusted-key

Use this command to define a “trusted” authentication key. If a key is trusted, the device will synchronize with a system that specifies this key in its NTP packets.

Use the no option with this command to remove a trusted key.

Command Syntax

```
ntp trusted-key <1-65534> (vrf management|)
no ntp trusted-key <1-65534> (vrf management|)
```

Parameter

<1-65534>	Authentication key number
management	Virtual Routing and Forwarding name

Default

By default, ntp trusted key is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp trusted-key 234676 vrf management
```

show ntp authentication-keys

Use this command to display authentication keys.

Command Syntax

```
show ntp authentication-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ntp authentication-keys
--------------------------
 Auth Key       MD5 String
--------------------------
123             0xa2cb891442844220
#
```

Table 8-12 explains the output fields.

Table 8-12: show ntp authentication-key fields

Entry	Description
Auth key	Authentication key (password). Use the password to verify the authenticity of packets sent from this interface or peer interface.
MD5 String	One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list.

show ntp authentication-status

Use this command to display whether authentication is enabled or disabled.

Command Syntax

```
show ntp authentication-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp authentication-status
Authentication enabled
```

show ntp logging-status

Use this command to display the NTP logging status.

Command Syntax

```
show ntp logging-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp logging-status
NTP logging enabled
```

show ntp peer-status

Use this command to display the peers for which the server is maintaining state along with a summary of that state.

Command Syntax

```
show ntp peer-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*216.239.35.4    .GOOG.           1 u   24   64  377   38.485    0.149   0.053
#
```

Table 8-13 explains the output fields.

Table 8-13: show ntp peer-status fields

Entry	Description
Total peers	Number of servers and peers configured.
* - selected for sync, + - peer mode (active), - - peer mode (passive), = - polled in client mode x - source false ticker	Fate of this peer in the clock selection process.
Remote	Address of the remote peer.
refid	Reference ID (0.0.0.0 for an unknown reference ID).
st	The stratum of the remote peer (a stratum of 16 indicated remote peer is unsynchronized).
t	Type of peer (local, unicast, multicast and broadcast).
when	Time the last packet was received.

Table 8-13: show ntp peer-status fields

Entry	Description
poll	The polling interval (seconds).
reach	The reachability register (octal).
delay	Current estimated delay in seconds.
offset	Current estimated offset in seconds.
jitter	Current dispersion of the peer in seconds.

show ntp peers

Use this command to display NTP peers.

Command Syntax

```
show ntp peers
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp peers
-------------------------------------------------------
Peer IP Address                          Serv/Peer
-------------------------------------------------------
216.239.35.4                             Server (configured)
```

Table 8-14 explains the output fields.

Table 8-14: show ntp peers fields

Entry	Description
Peer IP Address	Address of the neighbor protocol.
Serv/Peer	List of NTP peers and servers configured or dynamically learned.

show ntp statistics

Use this command to display NTP statistics.

Command Syntax

```
show ntp statistics (io | local | memory | peer ( ipaddr (A.B.C.D | X:X::X:X ) |
  name (HOSTNAME)) )
```

Parameters

`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation
`peer`	Counters associated with the specified peer
`A.B.C.D`	Peer IPv4 address
`X:X::X:X`	Peer IPv6 address
`HOSTNAME`	Peer host name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp statistics local
time since restart:     1685
time since reset:       1685
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0
bad length or format:   0
bad authentication:     0
rate exceeded:          0
#show ntp statistics memory
time since reset:     1698
total peer memory:    15
free peer memory:     15
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
```

Table 8-15 explains the output fields.

Table 8-15: show ntp statisticsfields

Entry	Description
Time since restart	Time when the ntp protocols were last started and how long they have been running.
Time since reset	Time when the ntp protocols were last reset and how long they have been running.
Packets received	Number of packets received from the peers.
Packets processed	Number of packets processed to the peers.
Current version	Current version of the protocol that is being used.
Previous version	Previous version of the protocol that has been used.
Declined	Access to the protocol declined
Access denied	Number of attempts denied to access protocol
Bad length or format	Number of messages received with length or format errors so severe that further classification could not occur.
Bad authentication	Number of messages received with incorrect authentication.
Rate exceeded	Exceed the configured rate if additional bandwidth is available from other queues
Total peer memory	Actual memory available to the peer system.
Free peer memory	Free memory available to the peer system.
Calls to find peer	Number of calls to find peer.
New peer allocations	Number of allocations from the free peer list.
Peer demobilizations	Number of structures freed to free peer list.
Hash table counts	Peer hash table’s each bucket count.

show ntp trusted-keys

Use this command to display keys that are valid for authentication.

Command Syntax

```
show ntp trusted-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp trusted-keys

Trusted Keys:
333
#
```

Table 8-16 explains the output fields.

Table 8-16: show ntp trusted-keys fields

Entry	Description
Trusted Keys	Keys that are valid for authentication.

show running-config ntp

Use this command to display the NTP running configuration.

Command Syntax

```
show running-config ntp (|all)
```

Parameters

`all`	Reserved for future use

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh running-config ntp
feature ntp vrf management
ntp enable vrf management
ntp authenticate vrf management
ntp logging vrf management
ntp authentication-key 123 md5 0xa2cb891442844220 7 vrf management
ntp trusted-key 123 vrf management
ntp server 216.239.35.4 vrf management
```

CHAPTER 9 Dynamic Host Configuration Protocol Relay

This chapter describes the Dynamic Host Configuration Protocol (DHCP) relay commands.

In small networks with only one IP subnet, DHCP clients communicate directly with DHCP servers. When DHCP clients and associated servers do not reside on the same subnet, a DHCP relay agent can be used to forward DHCP client messages to DHCP server.

The DHCP client broadcasts on the local link, the relay agents receives the broadcast DHCP messages, and then generate a new DHCP message to send out on another interface.

The relay agent sets the gateway IP address (`giaddr` field of the DHCP packet) and, if configured, adds the relay agent information option (option 82) in the packet and forwards it to the DHCP server. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

This chapter contains these commands:

ip dhcp relay (configure mode)

Use this command to enable the DHCP relay agent. The DHCP relay starts forwarding packets to the DHCP server address once configured.

Use the no form of this command to disable the DHCP relay agent.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

By default, this feature is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip dhcp relay

#configure terminal
(config)#no ip dhcp relay
```

ip dhcp relay (interface mode)

Use this command to configure an interface as a DHCP client-facing port.

Use the no form of this command to remove an interface as a DHCP client-facing port.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ip dhcp relay
```

ip dhcp relay address

Use this command to set an IPv4 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the no form of this command to remove the IP address of a DHCP server.

User must enable the DHCP relay feature with the ip dhcp relay (configure mode) command to configure server address.

Command Syntax

```
ip dhcp relay address A.B.C.D
no ip dhcp relay address A.B.C.D
```

Parameters

A.B.C.D	IPv4 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127

#configure terminal
(config)#ip dhcp relay address 198.51.100.127
```

ip dhcp relay information option

Use this command to enable the device to insert and remove option 82 information in DHCP packets forwarded by the relay agent.

The option 82 suboption remote-id can be configured either as hostname or any string provided by the User.

Use the no form of this command to disable inserting and removing option-82 information.

Command Syntax

```
ip dhcp relay information option (|remote-id (hostname|WORD))
no ip dhcp relay information option (|remote-id)
```

Parameters

remote-id	Remote host Identifier, can either be the System's hostname or a user-specified string.

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option remote-id hostname

#configure terminal
(config)#ip dhcp relay information option

#configure terminal
(config)#no ip dhcp relay information option
```

ip dhcp relay information source-ip

Use this command to enable DHCP relay option 82 link selection.

Use the no form of this command to disable DHCP relay option 82 link selection.

Command Syntax

```
ip dhcp relay information source-ip A.B.C.D
no ip dhcp relay information source-ip
```

Parameters

A.B.C.D	IPv4 address

Default

No default value is specified.

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option source-ip 2.2.2.2

#configure terminal
(config)#ip dhcp relay information option source-ip 3.3.3.3
```

ip dhcp relay uplink

Use this command to configure an interface as a DHCP server-facing port.

Use the no form of this command to remove an interface as a DHCP server-facing port.

Command Syntax

```
ip dhcp relay uplink
no ip dhcp relay uplink
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ip dhcp relay uplink
```

ipv6 dhcp relay (configure mode)

Use this command to enable the DHCP IPv6 relay agent.

Use the no form of this command to disable the DHCP IPv6 relay agent.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 dhcp relay

#configure terminal
(config)#no ipv6 dhcp relay
```

ipv6 dhcp relay (interface mode)

Use this command to configure an interface as a DHCPv6 client-facing port.

Use the no form of this command to remove an interface as a DHCPv6 client-facing port.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 dhcp relay
```

ipv6 dhcp relay address

Use this command to set an IPv6 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the no form of this command to remove an IPv6 address of a DHCP server.

User must enable the IPv6 DHCP relay feature with the ipv6 dhcp relay (configure mode) command to configure server address.

Command Syntax

```
ipv6 dhcp relay address X:X::X:X
no ipv6 dhcp relay address X:X::X:X
```

Parameters

X:X::X:X	IPv6 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F

#configure terminal
(config)#ipv6 dhcp relay address 2001:db8::7F
```

ipv6 dhcp relay uplink

Use this command to configure an interface as a DHCP IPv6 server-facing port.

Use the no form of this command to remove an interface as a DHCP IPv6 server-facing port.

Command Syntax

```
ipv6 dhcp relay uplink
no ipv6 dhcp relay uplink
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ipv6 dhcp relay uplink
```

show ip dhcp relay

Use this command to display DHCP relay status including DHCP server addresses configured on interfaces.

Command Syntax

```
show ip dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  Remote Id: ocnos-device
  Link selection Source-IP: 1.4.5.6
  DHCP Servers configured: 9.9.9.9 8.8.8.8
  Interface               Uplink/Downlink
  ---------               -------------
  ge10                    Uplink
  ge28                    Downlink
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  Link selection Source-IP: 1.2.3.4
  DHCP Servers configured: 1.1.1.1 2.2.2.2
  Interface               Uplink/Downlink
  ---------               -------------
  ge11                    Uplink
  ge27                    Downlink
```

show ip dhcp relay address

Use this command to display DHCP relay addresses.

Command Syntax

```
show ip dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured: 9.9.9.9 8.8.8.8
VRF Name: default
  DHCP Servers configured: 1.1.1.1 2.2.2.2
```

show ipv6 dhcp relay

Use this command to display DHCP IPv6 relay status including DHCP IPv6 server addresses configured on interfaces.

Command Syntax

```
show ipv6 dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge35                     Uplink
  xe50                     Downlink
VRF Name: default
  DHCPv6 Servers configured: 3001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge34                     Uplink
  xe49                     Downlink
```

show ipv6 dhcp relay address

Use this command to display DHCP IPv6 relay addresses.

Command Syntax

```
show ipv6 dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
VRF Name: default
  DHCPv6 Servers configured: 3001::1
```

show running-config dhcp

Use this command to display DHCP settings in the running configuration.

Command Syntax

```
show running-config dhcp
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show running-config dhcp
ip vrf vrf1
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 1.1.1.2

ip dhcp relay information option remote-id hostname
ip dhcp relay information source-ip 5.4.3.2
ip dhcp relay address 1.1.1.1
```

CHAPTER 10 Remote Management

This chapter is a reference for commands that copy these types of files:

- Start-up configuration and running configuration
- System files such as boot files, core dumps, and debug logs

You can use these commands to copy files locally or to copy between the local device and a remote system.

The commands in this chapter use the techniques in Table 10-17 to remotely transfer files:

Table 10-17: File transfer techniques

Trivial File Transfer Protocol (TFTP)	No authentication or encryption; dangerous to use over the Internet, but might be acceptable in a trusted environment Address format: `tftp:[//server[:port]][/path]`
File Transfer Protocol (FTP)	Authenticates, but does not encrypt Address format: `ftp:[//server][/path]`
Secure copy (SCP)	Authenticates and encrypts using Secure Shell (SSH1) Address format: `scp:[//server][/path]`
SSH File Transfer Protocol (SFTP)	Authenticates and encrypts using Secure Shell (SSH2); this is the most secure technique Address format: `sftp:[//server][/path]`
Hyper text Transfer Protocol (HTTP)	Address format: `http:[//server][/path]` For download of running and startup configurations

This chapter contains these commands.

copy running-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http HTTP-URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp sftp://sftp.mysite.com/running_conf vrf management
```

copy running-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp vrf management
```

copy startup-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http
  HTTP_URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp sftp://sftp.mysite.com/start-up_conf vrf management
```

copy startup-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp vrf management
```

copy system file

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy core myFile sftp sftp://sftp.mysite.com/dst_filename vrf management

#copy techsupport tech_support_23_Feb_2001_18_27_00.tar.gz scp scp://
10.12.16.17/home/satya/tech_support_23_Feb_2001_18_27_00.tar.gz vrf management
Enter Username:root
Enter Password:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
Copy Success
```

copy system file (interactive)

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy log myFile sftp sftp://sftp.mysite.com/dst_filename vrf management
```

copy ftp startup-config

Use this command to copy the start up configuration from an FTP server to the local device.

Command Syntax

```
copy ftp FTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`FTP-URL`	Configuration source: `ftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename startup-config vrf management
```

copy scp filepath

Use this command to copy the remote system file using SCP to the local device.

Note: OcNOS has a dedicated partition called `/cfg` for storing system level configurations, OcNOS configurations and license data. This is persistent across reboots and upgrades and consists of directories `/cfg/` and `/usr/local/etc`. Copying `user/general` files under `/cfg` partition is discouraged because the size of this partition is very small and impacts normal system operations like `bootup/upgrades` and important system files copy when it doesn't have enough space. Users are recommended to use `/home` to copy the general files. Please note that the contents placed in `/home` directory are deleted upon software upgrade.

Command Syntax

```
copy scp SCP-URL (filepath FILEPATH) (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`FILEPATH`	Enter the local filesystem path with filename
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 3.0.

Examples

```
#copy scp scp://10.12.65.89/root/cmlsh filepath /root/cmlsh vrf management
```

copy scp startup-config

Use this command to copy the start up configuration from a SCP server to the local device.

Command Syntax

```
copy scp SCP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp scp://scp.mysite.com/scr filename startup-config vrf management
```

copy sftp startup-config

Use this command to copy the start up configuration from a SFTP server to the local device.

Command Syntax

```
copy sftp SFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

SFTP-URL	Configuration source: sftp:[//server][/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp sftp://sftp.mysite.com/scr filename startup-config vrf management
```

copy tftp startup-config

Use this command to copy the start up configuration from a TFTP server to the local device.

Command Syntax

```
copy tftp TFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Configuration source: `tftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename startup-config vrf management
```

copy http startup-config

Use this command to copy the start up configuration from an HTTP server to the local device.

Command Syntax

```
copy http HTTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`HTTP-URL`	Configuration source: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http http://http.mysite.com/scr filename startup-config vrf management
```

copy ftp startup-config (interactive)

Use this command to copy the start up confguration from an FTP server to the local device.

Command Syntax

```
copy ftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp startup-config vrf management
```

copy scp startup-config (interactive)

Use this command to copy the start up confguration from a SCP server to the local device.

Command Syntax

```
copy scp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp startup-config vrf management
```

copy sftp startup-config (interactive)

Use this command to copy the start up confguration from an SFTP server to the local device.

Command Syntax

```
copy sftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp startup-config vrf management
```

copy tftp startup-config (interactive)

Use this command to copy the start-up confguration from a TFTP server to the local device.

Command Syntax

```
copy tftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp startup-config vrf management
```

copy http startup-config (interactive)

Use this command to copy the start-up confguration from an HTTP server to the local device.

Command Syntax

```
copy http startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http startup-config vrf management
```

copy file startup-config

Use this command to copy and store a local file into the startup configuration.

Command Syntax

```
copy file FILE startup-config
```

Parameters

FILE	File name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy file myFile startup-config
```

CHAPTER 11 Software Monitoring and Reporting

This document describes software watchdog and reporting related commands.

show tech-support

Use this command to collect system data for technical support.

Command Syntax

```
show tech-support
({bgp|cef|hw-info|isis|lacp|mpls|mstp|ospf|page|pim|rip|rsvp|tacacs+}|)
```

Parameters:

daemon	Protocol/daemon name

Default

The default file path for show techsupport is /var/log/.

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tech-support
#show tech-support bgp
#show tech-support bgp isis
```

CHAPTER 12 Source Interface Commands

This chapter is a reference for source interface commands. The source Interface feature routes management traffic to a dedicated interface using `iptables` NAT rules.

The source interface feature is supported for the protocols shown in Table 12-18.

Table 12-18: Source interface protocols and port numbers

Protocol	Default port number
Tacacs+	49
Radius	1812 and 1813
Snmp	161 and 162
Ntp	123
Syslog	514

Note: Because management applications are allowed only on the default and management VRF, the commands in this chapter are supported on the "management" and "default" VRFs only.

This chapter contains these commands:

- ip source-interface
- ipv6 source-interface
- show ip source-interface detail
- show ipv6 source-interface detail
- show running-config ip source-interface
- show running-config ipv6 source-interface

ip source-interface

Use this command to configure the IPv4 source interface for a protocol.

Use the no form of this command to remove the IPv4 source interface for a protocol.

Command Syntax

```
ip source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port <1025-65535>|)
  (vrf management|)
no ip source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port <1025-65535>|)
  (vrf management|)
```

Parameters

IFNAME	Interface name (lo or physical interface)
tacacs+	Terminal Access Controller Access Control System
ntp	Network Time Protocol
snmp	Simple Network Management Protocol
syslog	Rsyslog
radius	Remote Authentication Dial-In User Service
<1025-65535>	Port number. Default value is as per the protocol.
management	Virtual Routing and Forwarding name

Default

NA

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)# ip source-interface lo tacacs+
(config)# ip source-interface lo.management radius vrf management
(config)# ip source-interface xe1 syslog port 1025
(config)# ip source-interface lo.management ntp port 1026 vrf management
```

ipv6 source-interface

Use this command to configure the IPv6 source interface for a protocol.

Use the no form of this command to remove the IPv6 source interface for a protocol.

Command Syntax

```
ipv6 source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port <1025-65535>|)
  (vrf management|)
no ipv6 source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port <1025-
  65535>|) (vrf management|)
```

Parameters

IFNAME	Interface name (lo or physical interface)
tacacs+	Terminal Access Controller Access Control System protocol
ntp	Network Time Protocol
snmp	Simple Network Management Protocol
syslog	Rsyslog
radius	Remote Authentication Dial-In User Service
<1025-65535>	Port number. Default value is as per the protocol.
management	Virtual Routing and Forwarding name

Default

NA

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)# ipv6 source-interface lo tacacs+
(config)# ipv6 source-interface lo.management radius vrf management
(config)# ipv6 source-interface xe1 syslog port 1025
(config)# ipv6 source-interface lo.management ntp port 1026 vrf management
```

show ip source-interface detail

Use this command to display the IPv4 source interface status in detail.

Command Syntax

```
show ip source-interface detail
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ip source-interface detail
Source-Interface Detailed Information
=====================================
  Protocol : tacacs+
  Interface : lo
  Address : 1.1.1.1
  Status : Active
  VRF Name : Default

  Protocol : radius
  Interface : lo
  Address : 1.1.1.1
  Status : Active
  VRF Name : Default
```

Table 12-19 explains the output fields.

Table 12-19: Output fields

Field	Description
Protocol	tacacs+, ntp, snmp, syslog, or radius
Interface	Interface name (lo or physical interface)
Address	IP address
Status	Whether active or inactive
VRF Name	Virtual Routing and Forwarding name

show ipv6 source-interface detail

Use this command to display the IPv6 source interface status in detail.

Command Syntax

```
show ipv6 source-interface detail
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ipv6 source-interface detail
Source-Interface Detailed Information
=====================================
  Protocol : tacacs+
  Interface : lo
  Address : ::1
  Status : Active
  VRF Name : Default

  Protocol : radius
  Interface : lo
  Address : ::1
  Status : Active
  VRF Name : Default
```

Table 12-19 explains the output fields.

show running-config ip source-interface

Use this command to display the IPv4 source interface running configuration.

Command Syntax

```
show running-config ip source-interface
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0

Example

```
#show running-config ip source-interface
ip source-interface lo tacacs+ port 1025
ip source-interface lo radius
ip source-interface lo.management ntp vrf management
ip source-interface lo.management syslog port 1026 vrf management
ip source-interface ge3 snmp
```

show running-config ipv6 source-interface

Use this command to display the IPv6 source interface running configuration.

Command Syntax

```
show running-config ipv6 source-interface
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show running-config ipv6 source-interface
ip source-interface lo tacacs+ port 1025
ip source-interface lo radius
ip source-interface lo.management ntp vrf management
ip source-interface lo.management syslog port 1026 vrf management
ip source-interface ge3 snmp
```

Authentication Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Authentication, Authorization and Accounting

This chapter is a reference for the authentication:

- Authentication identifies users by challenging them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- Authorization provides a method of authorizing commands and services on a per user profile basis.

Note: Authorization will be auto-enabled if user enables the Authentication.

- Accounting collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The authentication feature allows you to verify the identity and, grant access to managing devices. The authentication feature works with the access control protocols as described in these chapters:

- Chapter 2, *RADIUS*
- Chapter 3, *TACACS+*

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter describes these commands:

- aaa authentication login default
- aaa accounting details
- aaa authentication login default
- aaa authentication login default fallback error
- aaa group server
- aaa local authentication attempts max-fail
- aaa local authentication unlock-timeout
- debug aaa
- server
- show aaa authentication
- show aaa authentication login
- show aaa groups
- show aaa accounting
- show running-config aaa

aaa authentication login

Use this command to set login authentication behavior.

Use the no form of this command to disable either authentication behavior.

Command Syntax

```
aaa authentication login error-enable (vrf management|)
no aaa authentication login error-enable (vrf management|)
```

Parameters

`error-enable`	Display login failure messages
`management`	Management VRF

Default

By default, aaa authentication login is local

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login error-enable vrf management
```

aaa accounting details

Use this command to set a list of server groups to which to redirect accounting logs.

Use the no form of this command to only log locally.

Command Syntax

```
aaa accounting default (vrf management|) ((group LINE)|local)
no aaa accounting default (vrf management|) ((group LINE)|local)
```

Parameters

group	Server group list for authentication
LINE	A space-separated list of up to 8 configured RADIUS or TACACS+ server group names
local	Use local authentication
management	Management VRF

Default

Default AAA method is local

Default groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa accounting default vrf management group radius
```

aaa authentication login default

Use this command to set the AAA authentication methods.

Use the no form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login default (vrf management|) ((group LINE) | (local (|none))
  | (none))
no aaa authentication login default (vrf management|) ((group LINE) | (local
  (|none)) | (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication
`management`		Management VRF

Default

By default, AAA authentication method is local

By default, groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the no form of this command to disable fallback to local authentication.

Command Syntax

```
aaa authentication login default fallback error local (vrf management|)
no aaa authentication login default fallback error local (vrf management|)
```

Parameters

management	Management VRF

Default

By default, AAA authentication is local.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

aaa group server

Use this command to create a server group and enter server group configure mode.

Use the no form of this command to remove a server group.

Command Syntax

```
aaa group server (radius|tacacs+) WORD (vrf management|)
no aaa group server (radius|tacacs+) WORD (vrf management|)
```

Parameters

`radius`	RADIUS server group
`tacacs+`	TACACS+ server group
`WORD`	Server group name; maximum 127 characters
`management`	Management VRF

Default

By default, the AAA group server option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa group server radius maxsmart
(config-radius)#
```

aaa local authentication attempts max-fail

Use this command to set the number of unsuccessful authentication attempts before a user is locked out.

Use the no form of this command to disable the lockout feature.

Command Syntax

```
aaa local authentication attempts max-fail <1-25>
no aaa local authentication attempts max-fail
```

Parameters

<1-25>	Number of unsuccessful authentication attempts

Default

By default, the maximum number of unsuccessful authentication attempts before a user is locked out is 3.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication attempts max-fail 2
```

aaa local authentication unlock-timeout

Use this command to set timeout value in seconds to unlock local user-account.

Use the no form of this command to set default timeout value in seconds.

Note: This command is applicable only to local user but not for user/s present at the server end to authenticate using TACACS+ or RADIUS.

Command Syntax

```
aaa local authentication unlock-timeout <1-3600>
no aaa local authentication unlock-timeout
```

Parameters

<1-3600>	Timeout in seconds to unlock local user-account. Default value is 1200.

Default

By default, the unlock timeout is 1200 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication unlock-timeout 1800
```

debug aaa

Use this command to display AAA debugging information.

Use the no form of this command to stop displaying AAA debugging information.

Command Syntax

```
debug aaa
no debug aaa
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug aaa
```

server

Use this command to add a server to a server group.

Use the no form of this command to remove from a server group.

Command Syntax

```
server (A.B.C.D | X:X::X:X | HOSTNAME)
no server (A.B.C.D | X:X::X:X | HOSTNAME)
```

Parameters

A.B.C.D	IPv4 address
X:X::X:X	IPv6 address

Default

None

Command Modes

RADIUS server group configure mode

TACACS+ server group configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+
(config)#aaa group server tacacs+ TacacsGroup4
(config-tacacs)#server 203.0.113.127
```

show aaa authentication

Use this command to display AAA authentication configuration.

Command Syntax

```
show aaa authentication (|vrf(management|all))
```

Parameters

None

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa authentication
                VRF: default
  default: local
  console: local
```

Table 1-20 explains the output fields.

Table 1-20: show aaa authentication fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.
Console	Authentication setting for the console access.

show aaa authentication login

Use this command to display AAA authentication configuration for login default and login console.

Command Syntax

```
show aaa authentication login error-enable (|vrf management|all))
```

Parameters

`error-enable`	Display setting for login failure messages
`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa authentication login error-enable
                VRF: default
disabled
```

Table 1-21 explains the output fields.

Table 1-21: show aaa authentication login error-enable fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show aaa groups

Use this command to display AAA group configuration.

Command Syntax

```
show aaa groups (vrf (management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa groups
VRF: default
radius
```

Table 1-22 explains the output fields.

Table 1-22: show aaa groups fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show aaa accounting

Use this command to display AAA accounting configuration.

Command Syntax

```
show aaa accounting (vrf (management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa accounting
                VRF: default
```

Table 1-23 explains the output fields.

Table 1-23: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show running-config aaa

Use this command to display AAA settings in the running configuration.

Command Syntax

```
show running-config aaa (vrf(management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa accounting
                VRF: default
  default: local
```

Table 1-24 explains the output fields.

Table 1-24: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.

CHAPTER 2 RADIUS

This chapter is a reference for Remote Authentication Dial In User Service (RADIUS) commands, RADIUS provides centralized Authentication, Authorization management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

- clear radius-server
- debug radius
- radius-server login host
- radius-server login host acct-port
- radius-server login host auth-port
- radius-server login host key
- radius-server login key
- radius-server login timeout
- show debug radius
- show radius-server
- show running-config radius

clear radius-server

Use this command to clear Radius Server statistics.

Command Syntax

```
clear radius-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
vrf	Virtual Routing and Forwarding
management	Management VRF
all	All VRF's

Default

No default value is specified

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
#clear radius-server counters vrf management
```

debug radius

Use this command to display RADIUS debugging information.

Use the no form of this command stop displaying RADIUS debugging information.

Command Syntax

```
debug radius
no debug radius
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug radius
```

radius-server login host

Use this command to configure a RADIUS server for both accounting and authentication.

Use the no form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num (<1-8>)|)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num (<1-8>)|) timeout <1-60>
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num (<1-8>)|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num (<1-8>)|) timeout
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of time out period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management
```

radius-server login host acct-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS accounting messages.

Use the no form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) acct-port <0-65535> |) | timeout <1-60> |)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) acct-port |) | timeout <1-60> |)
```

Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
seq-num	seq-num Sequence Number / Priority index for radius-servers
<1-8>	sequence number for servers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

By default, Radius-server login host acct-port is 1813

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 192.168.2.3 vrf management acct-port 23255
```

radius-server login host auth-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS authentication messages.

Use the no form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(auth-port <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) (auth-port (|(acct-port (|timeout))))
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`auth-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, Radius-server login host acct-port is 1812

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management auth-port 23255
```

radius-server login host key

Use this command to set per-server shared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a server shared key.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(key ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-
  port <0-65535> (|(timeout <1-60>))))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) (key ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-
  port (|(timeout)))))))
```

Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
seq-num	seq-num Sequence Number / Priority index for radius-servers
<1-8>	sequence number for servers
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management key 0 testing
auth-port 23255
```

radius-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a global preshared key.

Command Syntax

```
radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

Parameters

login	Remote login
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login key 7 p2AcxlQA vrf management

#configure terminal
(config)#no radius-server login key 7 p2AcxlQA vrf management
```

radius-server login timeout

Use this command to set the global timeout which is how long the device waits for a response from a RADIUS server before declaring a timeout failure.

Use the no form of this command to set the global timeout to its default (1 second).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
radius-server login timeout <1-60> (vrf management|)
no radius-server login timeout (vrf management|)
```

Parameters

`login`	Remote login
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Note: The system takes minimum 3 secs to timeout even though the configured timeout value is less than 3 seconds. Hence do not configure timeout value less than 3 secs. The timeout range value is mentioned as 1-60 secs for backward compatibility.

Default

By default, radius-server login timeout is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login timeout 15 vrf management

#configure terminal
(config)#no radius-server login timeout 15 vrf management
```

show debug radius

Use this command to display debugging information.

Command Syntax

```
show debug radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug radius
RADIUS client debugging is on
```

show radius-server

Use this command to display the RADIUS server configuration.

Command Syntax

```
show radius-server (|vrf(management|all))((WORD)|(groups (GROUP|)|)|sorted
```

Parameters

`WORD`	DNS host name or IP address
`groups`	RADIUS server group
`GROUP`	Group name; if this parameter is not specified, display all groups
`sorted`	Sort by RADIUS server name
`vrf`	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                          : 10.12.12.39
   Sequence Number                     : 1
   available for authentication on port : 1812
   available for accounting on port     : 1813
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :

Radius Server                          : 1.1.1.1
   Sequence Number                     : 2
   available for authentication on port : 1234
   available for accounting on port     : 1234
   timeout                             : 5
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :
```

Table 2-25 explains the output fields.

Table 2-25: show radius-server fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Timeout Value	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message
Total number of servers	Number of authentication requests received by the authentication server.

show running-config radius

Use this command to display RADIUS configuration settings in the running configuration.

Command Syntax

```
show running-config radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config radius
 10.12.12.39 vrf management seq-num 1 key 7 wawyanb123
 1.1.1.1 vrf management seq-num 2 auth-port 1234 acct-po
rt 1234
radius-server login key 7 wawyanb123
```

CHAPTER 3 TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+, usually pronounced like tack-axe) is an access control network protocol for network devices.

The differences between RADIUS and TACACS+ can be summarized as follows:

- RADIUS combines authentication and authorization in a user profile, while TACACS+ provides separate authentication.
- RADIUS encrypts only the password in the access-request packet sent from the client to the server. The remainder of the packet is unencrypted. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS is based on an open standard (RFC 2865). TACACS+ is proprietary to Cisco, although it is an open, publicly documented protocol (there is no RFC protocol specification for TACACS+).

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

clear tacacs-server counters

Use this command to clear the counter on a specified TACACS server.

Syntax

```
clear tacacs-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

HOSTNAME	The name of the server
X:X::X:X	IPv6 address of the server
A.B.C.D	IPv4 address of the server
vrf	VRF of the sever
management	The management VRF
all	All VRFs

Default

NA

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tacacs-server 10.1.1.1 counters
```

debug tacacs+

Use this command to display TACACS+ debugging information.

Use the no form of this command stop displaying TACACS+ debugging information.

Command Syntax

```
debug tacacs+
no debug tacacs+
```

Parameters

None

Default

Disabled

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug tacacs+
```

feature tacacs+

Use this command to enable the TACACS+ feature.

Use the no form of this command to disable the TACACS+ feature.

Command Syntax

```
feature tacacs+ (vrf management|)
no feature tacacs+ (vrf management|)
```

Parameters

`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, feature tacacs+ is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+ vrf management
```

show debug tacacs+

Use this command to display whether TACACS+ debugging is enabled.

Command Syntax

```
show debug tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug tacacs+
TACACS client debugging is on
```

show running-config tacacs+

Use this command to display TACACS+ settings in the running configuration.

Command Syntax

```
show running-config tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 7
0x9f4a8983e02
16052
```

Table 3-26 explains the output fields.

Table 3-26: show running-config fields

Entry	Description
TACAS server host	TACACS+ server Domain Name Server (DNS) name.
Seq-num	Sequence number of user authentication attempt with the TACACS+ server.
VRF Management	The management traffic using VPN Routing and Forwarding (VRFs).

show tacacs-server

Use this command to display the TACACS+ server configuration.

Command Syntax

```
show tacacs-server (|vrf (management|all))((WORD)|(groups (GROUP|)|)|(sorted)
```

Parameters

WORD	DNS host name or IP address
groups	TACACS+ server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by TACACS+ server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show tacacs-server
total number of servers:1

Tacacs+ Server                  : 192.168.10.215/49(*)
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 14
   Failed Connect Attempts      : 0
 Last Successful authentication: 2017 December 18, 12:27:13

(*) indicates last active.
```

Table 3-27 explains the output fields.

Table 3-27: show tacacs-server output fields

Field	Description
Sequence Number	Sequence number of user authentication attempt with the TACACS+ server.
Failed Auth Attempts	Number of times user authentication failed with the TACACS+ server. Increments for server key mismatches and password mismatches or wrong password for the user.
Success Auth Attempts	Number of times user authenticated with TACACS+ server. Increments for each successful login.

Table 3-27: show tacacs-server output fields

Field	Description
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server. Increments for server connection failure cases such as server not-reachable, server port mismatches.
Last Successful authentication	Timestamp when user successfully authenticated with the TACACS+ server.

tacacs-server login host

Use this command to set the TACACS+ server host name or IP address.

Use the no form of this command to remove an TACACS+ server (if only a host name or IP address is specified as a parameter) or to remove all of a TACACS+ server's configuration settings (if any other parameters are also specified).

Command Syntax

```
tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (seq-num
  <1-8> |) (key ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |)
no tacacs-server login host (HOSTNAME | A.B.C.D | X:X::X:X) (vrf management|)
no tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (key
  ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |)
```

Parameters

HOSTNAME	Host name
X:X::X:X	IPv6 address
A.B.C.D	IPv4 address
vrf	Virtual Routing and Forwarding
management	Management VRF
seq-num	Sequence Number / Priority index for tacacs-servers
key	Authentication and encryption key ("shared secret")
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
port	TACACS+ server port
<1205-65535>	TACACS+ server port number; the default is 49

Default

Enable authentication for TACACS+ server configured. Authorization is also enabled by default. The default server port is 49.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login host 203.0.113.31 vrf management
```

tacacs-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and TACACS+ servers.

Use the no form of this command to remove a global preshared key.

Command Syntax

```
tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

Parameters

0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login key 7 jvn05mlQH1 vrf management
```

tacacs-server login timeout

Use this command to set the period to wait for a response from the server before the client declares a timeout failure. The default timeout value is 5 seconds.

You can only give this command when the TACACS+ feature is enabled.

Use the `no` form of this command to set the timeout value to its default value (5 seconds).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
tacacs-server login timeout <1-60> (vrf management|)
no tacacs-server login timeout (vrf management|)
```

Parameters

`<1-60>`	Timeout value in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#tacacs-server login timeout 35 vrf management
```

SECTION 3

Security Features

Security Features Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Proxy ARP and Local Proxy ARP

Overview

Proxy ARP (RFC 1027) is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address as destination. The captured traffic is then typically routed by the Proxy to the intended destination via another interface. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

Use `no ip proxy-arp` to disable Proxy ARP, Proxy ARP is disabled by default.

Topology

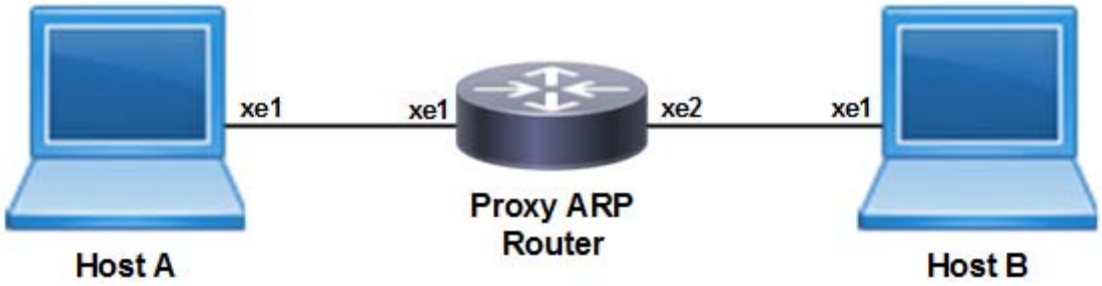


Figure 1-28: Sample topology

Host A

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured on Host A
`(config-if)#ip address 20.20.0.2/16`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter Configure mode
`(config)#interface xe1`	Specify the interface to be configured on Host B
`(config-if)#ip address 20.20.1.2/24`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Enable Proxy ARP

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface connected to Host A
`(config-if)#ip address 20.20.0.1/24`	Configure the ip address on the interface
`(config-if)#interface xe2`	Specify the interface connected to Host B
`(config-if)#ip address 20.20.1.1/24`	Configure the ip address on the interface
`(config-if)#interface xe1`	Specify the interface to configure Proxy ARP
`(config-if)#ip proxy-arp`	Enable Proxy ARP
`(config)#end`	Exit interface and configure mode

Validation

```
#show running-config arp
!
interface xe1
ip proxy-arp
!
```

The `show arp` command on the hosts shows the arp table entries to reach different subnets. Ping Host B from Host A.Host A. The ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State
20.20.0.3      00:02:39      ecf4.bbc0.3d71      xe1       STALE.
```

Local Proxy ARP Overview

Local Proxy ARP feature is used to enable local proxy support for ARP requests per interface level. Activation will make the router answer all ARP requests on configured subnet, even for clients that should not normally need routing. Local proxy ARP means that the traffic comes in and goes out the same interface.

The local proxy ARP feature allows responding to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

Topology

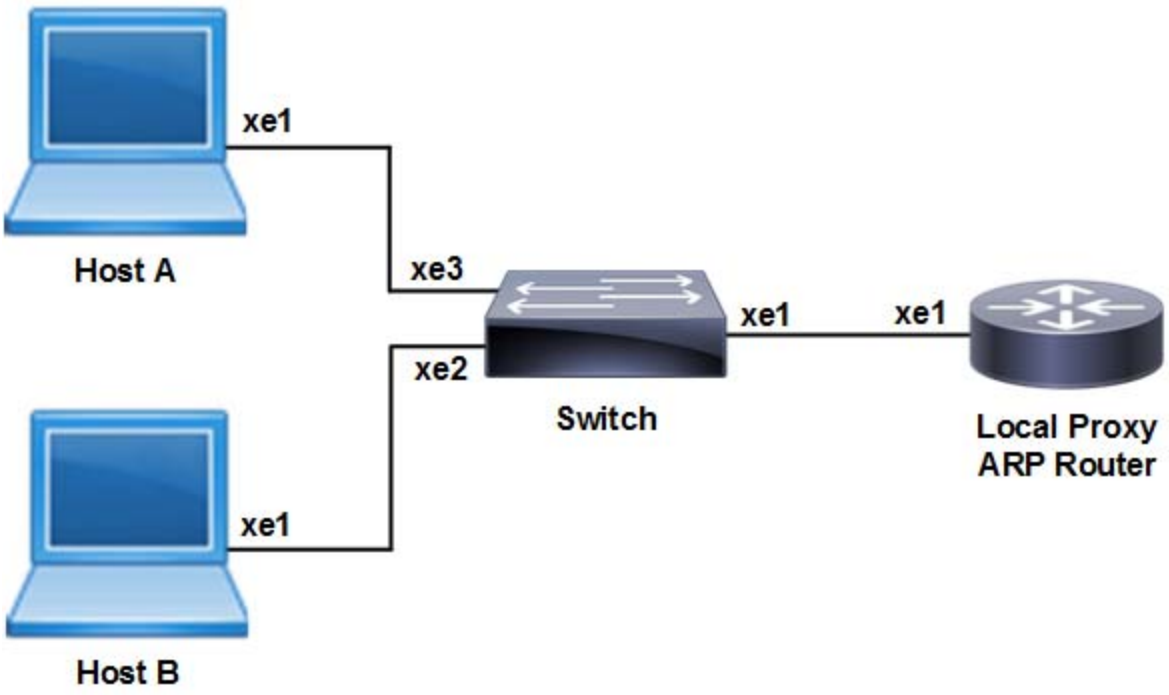


Figure 1-29: Sample topology

Host A

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured on Host A
`(config-if)#ip address 20.20.0.2/16`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter Configure mode
`(config)#interface xe1`	Specify the interface to be configured on Host B
`(config-if)#ip address 20.20.0.3/24`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Private Vlan Configuration on Switch

`#configure terminal`	Enter Configure mode.
`(config)# bridge 1 protocol ieee vlan-bridge`	Create ieee vlan-bridge on switch for pvlan configuration
`(config)# vlan database`	Enter into the vlan database
`(config-vlan)# vlan 100-101 bridge 1 state enable`	Create vlans 100 and 101 as part of bridge 1
`(config-vlan)# private-vlan 100 primary bridge 1`	Configure vlan 100 as a primary vlan
`(config-vlan)# private-vlan 101 isolated bridge 1`	Configure vlan 101 as a isolated vlan
`(config-vlan)# private-vlan 100 association add 101 bridge 1`	Associate secondary vlan 101 to primary vlan 100
`(config-vlan)#exit`	Exit from the vlan database
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#switchport`	Configure xe1 as a layer2 interface.
`(config-if)#bridge-group 1`	Associate the interface to the bridge
`(config-if)#switchport access vlan 100`	Associate primary vlan to the interface
`(config-if)#switchport mode private-vlan promiscuous`	Configure xe1 interface as a promiscuous port
`(config-if)# switchport private-vlan mapping 100 add 101`	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
`(config-if)# exit`	Exit interface mode
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#switchport`	Configure xe2 as a layer2 interface.
`(config-if)#bridge-group 1`	Associate the interface to the bridge
`(config-if)#switchport access vlan 100`	Associate primary vlan to the interface
`(config-if)#switchport mode private-vlan promiscuous`	Configure xe2 interface as a promiscuous port
`(config-if)# switchport private-vlan mapping 100 add 101`	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
`(config-if)# exit`	Exit interface mode
`(config)#interface xe3`	Specify the interface to be configured
`(config-if)#switchport`	Configure xe3 as a layer2 interface.

(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe2 interface as a promiscuous port
(config-if)# switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)# exit	Exit interface mode

Enable Local Proxy ARP on Router

#configure terminal	Enter Configure mode
(config)#interface xe1	Specify the interface to be configured on Host B
(config-if)#ip address 20.20.0.3/24	Configure the ip address on the interface
(config-if)#ip local-proxy-arp	Enable Local Proxy ARP
(config)#end	Exit interface and configure mode

Validation

ARP cache on Host A and Host B

The show arp command on hosts shows the arp table entries to reach different subnets. Ping Host B from Host A.Host A ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State
20.20.0.3      00:02:39      ecf4.bbc0.3d71      xe1       STALE.
```

SECTION 4

System Configuration

Control Plane Policing Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Control Plane Policing Configuration

Control plane policing (CoPP) manages the traffic flow destined to the host router CPU for control plane processing. CoPP limits the traffic forwarded to the host CPU and avoids impact on system performance.

1. CoPP has organized handling of control packets by providing per-protocol hardware CPU queues. So, control packets are queued in different CPU queues based on protocol.
2. Per-protocol CPU queue rate limits and buffer allocations are programmed during router initialization, thus every CPU queue is rate-limited to a default stable and balanced behavior across protocols.
3. When control packets received at higher rate than the programmed rate, the excess traffic is dropped at queue level in the packet processor hardware itself.
4. OcNOS does not support per-queue rate modification and usage monitoring.
5. All CPU queues are pre-programmed with default rate limits and buffer allocations to ensure a default stable and balanced behavior across protocols.
6. Rate limits are in terms of kbps. Hardware does not support PPS (packets per second).
7. Qumran (MX, AX, and UX) supports per-queue rate shaping configuration within a range of 469 kbps to 483 gbps. The granularity is 469 kbps for low range and 1.56% for higher range.

.

Table 1-28: Default CPU queues

Default queues	Default rate In kbps	Maximum configurable rate in kbps	Default queue length In kbytes	Description
CPU0.q0	900	900	1024	Unclassified protocols and unknown or destination lookup failure packets are redirected to default CPU queues 0-7 based on packet's cos/dscp values. SSH, TELNET and SNMP traffic destined to host router CPU is remarked to CPU0.q6. SSH: TCP Source/Destination port 22 TELNET: TCP Source/Destination port 23 SNMP: UDP Source/Destination port 161/162
CPU0.q1	900	900	1024	
CPU0.q2	900	900	1024	
CPU0.q3	900	900	1024	
CPU0.q4	900	900	1024	
CPU0.q5	900	900	1024	
CPU0.q6	900	900	1024	
CPU0.q7	900	900	1024	
CPU1.q0	900	900	1024	
CPU1.q1	900	900	1024	
CPU1.q2	900	900	1024	
CPU1.q3	900	900	1024	
CPU1.q4	900	900	1024	
CPU1.q5	900	900	1024	
CPU1.q6	900	900	1024	
CPU1.q7	900	900	1024	
*cpu1 is valid only for QMX				

Table 1-29: Per protocol CPU queues

Protocol queues	Default rate In kbps	Maximum configurable Rate in kbps	Default queue length In kbytes	Description
IGMP	1000	1000	2048	Internet Group Management Protocol packets (IP protocol 2)
ISIS/ESIS	8000	8000	1024	ISIS (DMAC 0180:C200:0014/0015) ESIS (DMAC 0900:2B00:0004/0005) Note: ESIS = End System-to-Intermediate System (ISIS point-to-point case)
Reserved Mcast	8000	8000	2048	Reserved IPv4 and IPv6 Multicast packets IPv4: Local Network Control Block (224.0.0.0 - 224.0.0.255 (224.0.0/24)) IPv6: Link-Local Scope Multicast Addresses (FF02::/8)
IPv6 Link Local	1000	1000	1024	IPv6 link local packets DIPv6: FE80::/8

Table 1-29: Per protocol CPU queues (Continued)

Protocol queues	Default rate In kbps	Maximum configurable Rate in kbps	Default queue length In kbytes	Description
ospf	8000	8000	1024	OSPF unicast packets (IP protocol 89)
bgp	8000	8000	1024	BGP packets TCP source/destination port number: 179
rsvp/ldp	2000	2000	1024	RSVP and LDP packets RSVP: IP protocol 46 LDP: L4 source/destination port number:646
vrrp/rip/ dhcp	8000	8000	1024	VRRP packets: IP protocol number 112 RIP packets: UDP source and destination port number: 520 RIPNG packets: UDP source and destination port number: 521 DHCP: DHCP v4/v6 server packets, DHCP v4/v6 client packets (L4 source/destination port number: 67 or 68)
pim	1000	1000	1024	Protocol Independent Multicast packets: IP protocol number 103
icmp	1000	1000	1024	ICMP packets: IP protocol number 1 Unicast ICMPv6 packets: IP next header number 58
arp	1000	1000	1024	ARP packets. Ether-type 0x0806
bpdu	1000	1000	1024	xSTP: DMAC 0180:C200:0000 Provider Bridging: 0180:C200:0008 LACP: DMAC 0180:C200:0002, ethertype:0x8809, subtype:1/2 AUTHD: DMAC 0180:C200:0003 LLDP: DMAC 0180:C200:000E EFM: DMAC 0180:C200:0002, ethertype:0x8809, subtype:3 ELMI: DMAC 0180:C200:0007 SYNCE: DMAC 0180:C200:0002, ethertype:0x8809, subtype:0x0A RPVST: DMAC 0100:0CCC:CCCD L2TP: DMAC 0100:C2CD:CDD0/0104:DFCD:CDD0 G8032: DMAC 0119:A700:00XX
bfd	16384	16384	1024	BFD Single hop packets: UDP port 3784, TTL 255 BFD Multi hop packets: UDP port 4784 Micro BFD packets: UDP port 6784, TTL 255
sflow	1500	1500	1024	Ingress and Egress sampled packets
dsp	500	500	76800	L2 FDB events
vxlan	500	500	1024	ARP and ND cache queue for packets coming on VXLAN access ports.
nhop	400	400	1024	Inter VRF route leak unresolved data packets for ARP resolution.
icmp-redirect	1000	1000	256	Data packets to CPU for ICMP redirect packet generation.

Hybrid Switch Router Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Hybrid Switching Overview

An OcNOS Hybrid Switch Router offers Layer 3 forwarding found in routers with the high-speed performance associated with traditional Layer 2 switches. The following are some advantages of Hybrid Switch Routers:

- Reduced system cost and infrastructure. Traditionally you would require a separate box for switching and one for routing.
- Off-loading IP traffic from backbone routers, thus making them more efficient for firewalls and WAN connectivity.
- Simplified network design and maintenance.

Routing and Switching

Layer 2 and Layer 3 switches are similar at a high-level, both look at the packet headers, and steer the packets toward their destination port. Therefore, after being passed through a switch or router, the packet is closer to its destination.

Layer 2 Switching

Layer 2 switches are typically used to provide connectivity within high bandwidth local area networks (LANs). A Layer 2 switch makes forwarding decisions based on the MAC or the Layer 2 header. It extracts the Layer 2 header from the packet, finds a matching destination address in the forwarding table, and transmits the packet out to the port associated with the specific destination address in the forwarding table. The forwarding table is populated through a self-learning process, whereby each arriving packet is used to update the entries in the table. Typically, the Layer 2 switch implements the switching function in the hardware, as that requires stripping of the packet only in two layers (the physical and data link layer) to get to the useful part of the packet header. This allows switches to steer packets at wire-speed rates without slowing down arriving streams of packets to process them.

Layer 3 Routing

Layer 3 (L3) routers are typically used to provide connectivity between different LANs. A Layer 3 router discards MAC headers, and indexes further into the packet–making decisions based on the IP or Layer 3 header. It extracts the Layer-3 header from the packet, finds a matching destination address in a routing table, identifies a new MAC address for the packet from an ARP cache, wraps the IP packet in a new MAC header, and then transmits the packet out to the port associated with that destination address in the routing table.

The routing table is populated through statically configured command line interface entries or through routing protocol messages from neighboring routers. A Layer 3 router must strip through 3 layers (physical, data link, and network) which is more complicated than a Layer 2 switch. Layer 3 routers historically implement the routing function in software. This often results in limited packet-forwarding rates. However, improvements in VLSI circuit technology have allowed Layer 3 routing functions to be implemented rapidly in hardware, enabling wire-speed performance similar to the performance of Layer 2 switches. As a result, along with the complexity of next-generation Layer 3 routers, the throughput of these routers has also been increasing.

An architecture is required that is flexible enough to accommodate the demands of different customers, and accommodate the changing demands of a single customer whose requirements may change over time. Typical Layer 2 switches and Layer 3 routers fail to provide this flexibility.

An optimal configuration can be an integrated solution, a Layer 3 router with Layer 2 bridge groups around it. The OcNOS Hybrid Switch Router implementation allows easy configuration of different combinations of routers and switches. OcNOS can be configured as an absolute Layer 3 router, absolute Layer 2 switch (Figure 1-30) or a hybrid Layer 2/Layer 3 switch router, (Figure 1-31) that can easily change modes with the use of a single command.

System Configuration

- OcNOS stack will bring up all the ports of the board as routed ports by default.
- However OcNOS provides flexibility to create a Layer 2 bridge, and ports can be converted to switch ports and added to the bridge.
- OcNOS also supports VLAN interfaces and routing between VLANs.

Thus it can work as a router, a switch, or as a hybrid switch.

Hybrid Switch Router Possibilities

With only Layer 2 protocols configured, the OcNOS Hybrid Switch Router can become an absolute Layer 2 switch.

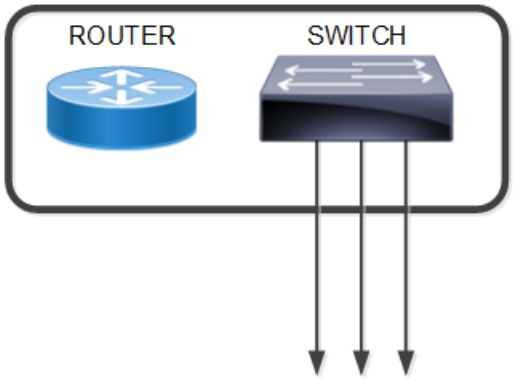


Figure 1-30: Layer 2 Switch

With Layer 2 and Layer 3 protocols configured, the OcNOS Hybrid Switch Router can become a Switch and/or a Router.

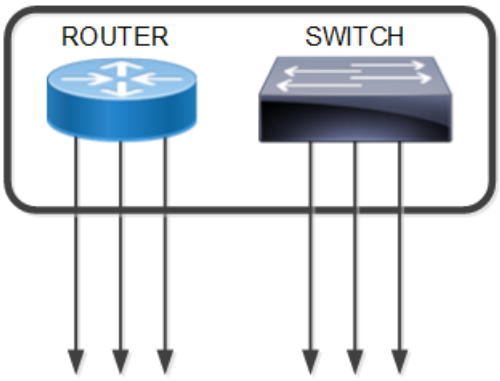


Figure 1-31: Working as a Router or a Switch

With only Layer 3 protocols enabled, the OcNOS Hybrid Switch Router can become an absolute router.

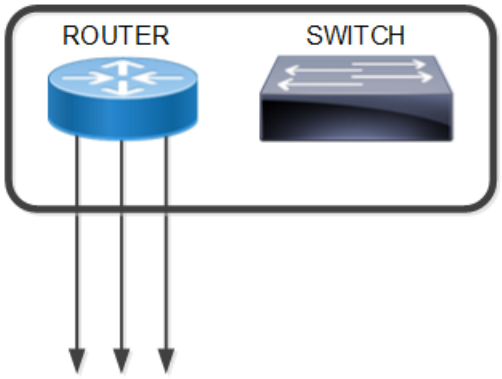


Figure 1-32: Working as Layer 3 Router

On switch ports, VLANs can be created for different broadcast domains.

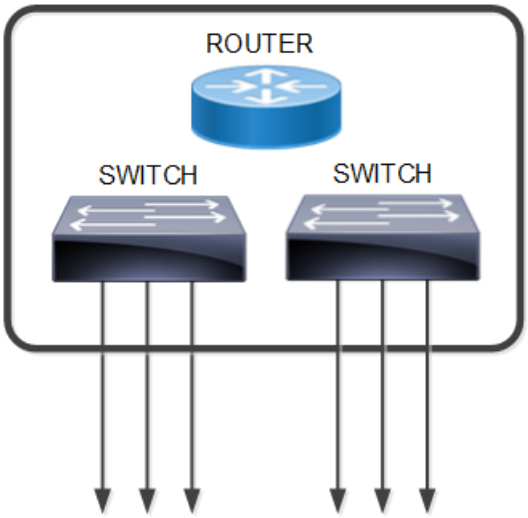


Figure 1-33: Port- or Policy-based VLANs

For routing between VLANs, the OcNOS routing protocols or static routing via NSM can be utilized.

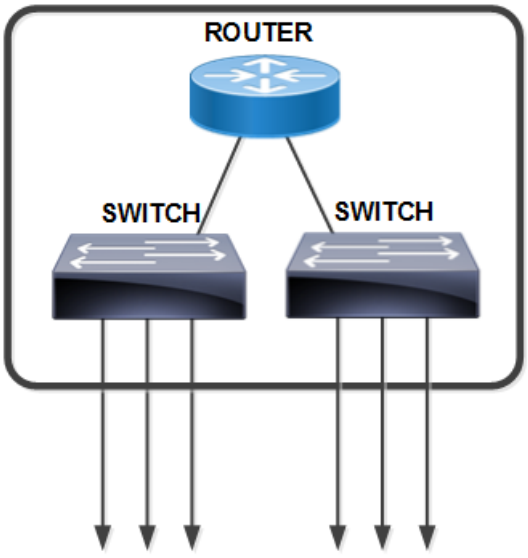


Figure 1-34: Routing between VLANs

For routing between VLANs and other routing ports, OcNOS routing protocols or static routing via NSM can be utilized.

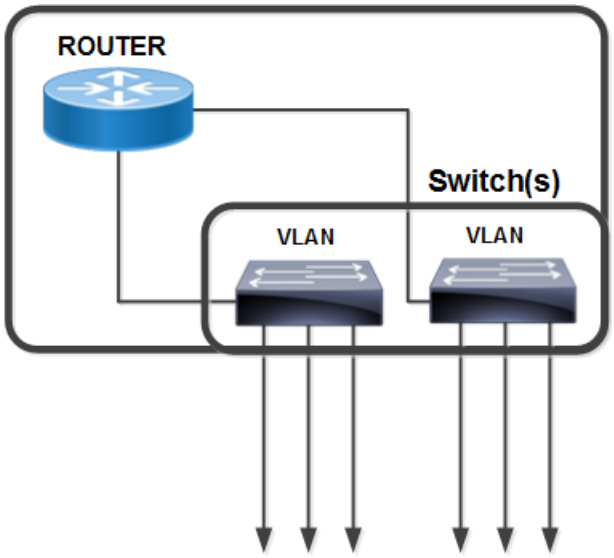


Figure 1-35: Routing between VLANs and Routing Ports

CHAPTER 2 Hybrid Switch Router Configuration

This chapter describes various configurations that can be done with the Hybrid Switch Router solution. OcNOS can be configured as a Layer 2 switch, a Layer 3 router or a Hybrid Switch Router.

Configuring Layer 2 Interfaces

For the Hybrid Switch Router, it is important to understand that by default, all interfaces are configured as routed interfaces. To configure a Layer 2 interface (switched interface), you must explicitly configure this using the `switchport` command in the interface mode. For example:

`#configure terminal`	Enter the Configure mode.
`(config)#bridge 1 protocol mstp`	Create a MSTP bridge.
`(config)#interface eth2`	Specify an interface to configure and enter the Interface mode.
`(config-if)#switchport`	Configure eth2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate interface to bridge 1.
`(config-if)#no shutdown`	Start interface.eth2

Configuring Layer 3 Interfaces

For the Hybrid Switch Router, it is important to understand that by default, all interfaces in OcNOS are L3 ports. If a port has been configured as L2, then use the `no switchport` command to make it a L3 port.

For example:

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth3`	Specify an interface to configure and enter the Interface mode.
`(config-if)#no switchport`	Configure eth3 as a Layer 3 port.

In the Hybrid Switch Router mode, if a VLAN is configured, a Layer 3 interface based on the bridge-group number and VLAN ID is created. This Layer 3 interface is advertised to all the Layer 3 protocols. For example:

`#configure terminal`	Enter the Configure mode.
`(config)#bridge 1 protocol mstp`	Creating bridge.
`(config)#vlan database`	Enter the VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1`	Enable VLAN 2 on bridge 1.

The last step in the example above show an interface given a name with the following format:

```
vlanXX.YYYY
```

Where XX is the bridge ID, and YYYY is the VLAN ID,

For example, the name, `vlan1.3` indicates that VLAN IP's interface is in VLAN 3, and bridge-group 1.

Integrated Management Interface Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Common IMI Commands

This chapter describes common Integration Management Interface (IMI) commands.

- show users
- terminal width
- terminal length
- terminal monitor
- write

banner motd

Use this command to set the message of the day (motd) at login.

After giving this command, you must write to memory using the terminal monitor command. If you do not write to memory, the new message of the day is not available after the device reboots.

Use the no parameter to not display a banner message at login.

Command Syntax

```
banner motd LINE
banner motd default
no banner motd
```

Parameters

LINE	Custom message of the day.
default	Default message of the day.

Default

By default, the following banner is displayed after logging in:

```
OcNOS version 1.3.4.268-DC-MPLS-ZEBM 09/27/2018 13:44:22
```

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#banner motd default

#configure terminal
(config)#no banner motd
```

configure terminal

Use this command to enter configure mode.

Command Syntax

```
configure terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering configure mode (note the change in the command prompt).

```
#configure terminal
(config)#
```

configure terminal force

Use the configure terminal force command to kick out the configure command mode to privileged EXEC mode, iff there is any session already in configure command mode.

Note: Configure terminal force with option 0 or without any option indicates immediate kick out the session which is locked to configure command mode. similarly, configure terminal force with option of any value indicates session locked to configure command mode will be exited to privileged Exec mode after the specified number of seconds completed.

Command Syntax

```
configure terminal force <0-600|>
```

Parameters

<0-600>	Timeout value in seconds for the session in config mode to exit to Privileged

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal force 0
#
```

copy running-config startup-config

Use this command to a write the configuration to the file used at startup. This is the same as the terminal monitor command.

Command Syntax

```
copy running-config startup-config
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```

disable

Use this command from to exit privileged exec mode and return to exec mode. This is the only command that allows you to go back to exec mode. The exit or quit commands in privileged exec mode end the session without returning to exec mode.

Command Syntax

```
disable
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#disable
>
```

enable

Use this command to enter privileged exec command mode.

Command Syntax

```
enable
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering the Privileged Exec mode (note the change in the command prompt).

```
>enable
#
```

enable password

Use this command to change or create a password to use when entering enable mode.

Note: Only network administrators can execute this command. For more, see the username command.

There are three methods to enable a password:

Plain Password

The plain password is a clear text string that appears in the configuration file as configured.

Encrypted Password

An encrypted password encrypts a password. First, use this command to create a password. Then, use the service password-encryption command to encrypt the password. An encrypted password does not display in the configuration file; instead, it displays the encrypted string.

Hidden Password

A hidden password also encrypts a password; however, you do not need the service password-encryption command for this method. Use this method if you know the encrypted string of the plain text string that you want to use as a password. The output in the configuration file displays only the encrypted string and not the text string.

Use the no parameter to disable the password.

Command Syntax

```
enable password (8|) LINE
no enable password
no enable password LINE
```

Parameters

8	Hidden password.
line	Password string, up to 80-characters, including spaces. The string cannot begin with a number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#enable password mypasswd
```

end

Use this command to return to privileged exec command mode from any other advanced command mode.

Command Syntax

```
end
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows returning to privileged exec mode directly from interface mode.

```
#configure terminal
(config)#interface eth0
(config-if)#end
#
```

exec-timeout

Use this command to set the interval the command interpreter waits for user input detected. That is, this sets the time a telnet session waits for an idle VTY session before it times out. A value of zero minutes and zero seconds (0 and 0) causes the session to wait indefinitely.

Use the no parameter to disable the wait interval.

Command Syntax

```
exec-timeout <0-35791> (<0-2147483>|)
no exec-timeout
```

Parameters

<0-35791>	Timeout value in minutes.
<0-2147483>	Timeout value in seconds.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the telnet session will timeout after 2 minutes, 30 seconds if there is no response from the user.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#exec-timeout 2 30
```

exit

Use this command to exit the current mode and return to the previous mode. When used in exec mode or privileged exec mode, this command terminates the session.

Command Syntax

```
exit
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows exiting interface mode and returning to configure mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
(config)#
```

help

Use this command to display help for the OcNOS command line interface.

Command Syntax

```
help
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
```

history

Use this command to set the maximum number of commands stored in the command history.

Use the no parameter to remove the configuration.

Command Syntax

```
history max <0-2147483647>
no history max
```

Parameters

`<0-2147483647>` Number of commands.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#line vty 12 77
(config-line)#history max 123

(config-line)#no history max
```

hostname

Use this command to set the network name for the device. OcNOS uses this name in system prompts and default configuration filenames.

Setting a host name using this command also sets the host name in the kernel.

Note: After giving the `hostname` command, you must write to memory using the terminal monitor command. If you do not write to memory, the change made by this command (the new host name) is not set after the device reboots.

Use the `no` parameter to disable this function.

Command Syntax

```
hostname WORD
no hostname (WORD|)
```

Parameter

`WORD`	Network name for a system. Per RFC 952 and RFC 1123, a host name string can contain only the special characters period (“.”) and hyphen (“-”). These special characters cannot be at the start or end of a host name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#hostname ABC
(config)#

(config)#no hostname
(config)#exit
```

line console

Use the this command to move or change to the line console mode.

Command Syntax

```
line console <0-0>
```

Parameters

<0-0>	First line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example enters line mode (note the change in the prompt).

```
#configure terminal
(config)#line console 0
(config-line)#
```

line vty (all line mode)

Use this command to move or change to all line VTY mode.

Note: line vty is just a mode changing command, and it can't exist without sub attributes being configured. i.e exec-timeout.

Command Syntax

```
line vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
(config)#
```

line vty (line mode)

Use this command to move or change to VTY mode. This command is used to connect to a protocol daemon. This configuration is necessary for any session. This configuration should be in the daemon's config file before starting the daemon.

Use the no parameter to disable this command.

Note: line vty is just a mode changing command, and it can't exist without sub attributes being configured. i.e exec-timeout.

Command Syntax

```
line vty <0-871> <0-871>
no line vty <0-871> (<0-871>|)
```

Parameters

<0-871>	Specify the first line number.
<0-871>	Specify the last line number.

Note: Configurations (exec-timeout) performed under this mode, affects only the current VTY session.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty 9
(config-line)#exit
(config)no line vty 9
```

logging cli

Use this command to enable logging commands entered by all users.

Use the no parameter to disable logging commands entered by all users.

Command Syntax

```
logging cli
no logging cli
```

Parameter

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging cli
(config)#no logging cli
```

logout

Use this command to exit from the shell from any exec mode.

Command Syntax

```
logout
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show the use of `logout` command.

```
>logout
OcNOS login:

>enable
en#logout
>
```

quit

Use this command to exit the current mode and return to the previous mode. When this command is executed in one of the exec modes, it closes the shell and logs you out.

Command Syntax

```
quit
```

Parameters

None

Default

No default value is specified

Command Mode

All modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#

>enable
#quit
[root@TSUP-123 sbin]#
```

service advanced-vty

Use this command to set multiple options to list when the tab key is pressed while entering a command. This feature applies to commands with more than one option.

Use the no parameter to not list options when the tab key is pressed while entering a command.

Command Syntax

```
service advanced-vty
no service advanced-vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#service advanced-vty
(config)#no service advanced-vty
```

service password-encryption

Use this command to encrypt passwords created with the enable password command. Encryption helps prevent observers from reading passwords.

Use the no parameter to disable this feature.

Command Syntax

```
service password-encryption
no service password-encryption
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#enable password mypasswd
(config)#service password-encryption
```

service terminal-length

Use this command to set the number of lines that display at one time on the screen for the current terminal session.

Use the no parameter to disable this feature.

Command Syntax

```
service terminal-length <0-512>
no service terminal-length (<0-512>|)
```

Parameters

<0-512>	Number of lines to display. A value of 0 prevents pauses between screens of output.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service terminal-length 60
```

show clock

Use this command to display the current system time.

Command Syntax

```
show clock
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show clock
12:54:02 IST Fri Apr 29 2016
```

show cli history

Use this command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

Command Syntax

```
show cli history
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show cli history
   1 en
   2 show ru
   3 con t
   4 show spanning-tree
   5 exit
```

show logging cli

Use this command to display command history for all users.

Command Syntax

```
show logging cli ((logfile LOGFILENAME)|) (match-pattern WORD |)
show logging cli last <1-9999>
show logging logfile list
```

Parameters

LOGFILENAME	Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.
WORD	Display only lines with this search pattern.
<1-9999>	Number of lines to display from the end of the command history.
logfile list	Display a list of command history files.

Default

LOGFILENAME Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh logging cli
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#show logging cli last 2
2017 Mar 1 16:34:26.302 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging info'
2017 Mar 1 16:34:37.317 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging cli last 2'
#show logging logfile list
file1
file2
```

show process

Use this command to display the OcNOS daemon processes that are running.

Command Syntax

```
show process
```

Parameters

None

Command Mode

Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show process
 PID NAME             TIME     FD
   1 nsm          00:56:29     7
   2 ripd         00:56:29     11
   3 ripngd       00:56:29     12
   4 ospfd        00:56:29     9
   5 ospf6d       00:56:29     10
   6 bgpd         00:56:29     14
   9 isisd        00:56:29     8
#
```

Table 1-30 explains the output fields.

Table 1-30: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S)—Number of system and user CPU seconds that the process has used. (None, D, and E)—Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.

show running-config

Use this command to show the running system status and configuration.

Command Syntax

```
show running-config
show running-config full
```

Parameters

`full`	Display the full configuration information.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config
no service password-encryption
!
no service dhcp
ip domain-lookup
!
mpls propagate-ttl
!
vrrp vmac enable
spanning-tree mode provider-rstp
no data-center-bridging enable
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.1.2.173/24
 no shutdown
!
interface eth1
 shutdown

!
line con 0
 login
!
end
(config)#
```

show running-config access-list

Use this command to show the running system status and configuration details for access lists.

Command Syntax

```
show running-config access-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config access-list
!
access-list abc remark annai
access-list abc deny any
access-list abd deny any
!
#
```

show running-config as-path access-list

Use this command to show the running system status and configuration details for access lists based on autonomous system paths.

Command Syntax

```
show running-config as-path access-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config as-path access-list
!
ip as-path access-list wer permit knsmk
!
(config)#
```

show running-config community-list

Use this command to show the running system status and configuration details for community lists.

Command Syntax

```
show running-config community-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
(config)#show running-config community-list
!
ip community-list standard aspd permit internet
ip community-list expanded cspd deny ljj
ip community-list expanded cspd permit dcv
ip community-list expanded wde permit njhd
ip community-list expanded wer deny sde
(config)#
```

show running-config interface igmp

Use this command to show the running system status and configuration for IGMP.

Command Syntax

```
show running-config interface IFNAME ip igmp
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
!
```

show running-config interface multicast

Use this command to show the running system status and configuration for a multicast interface.

Command Syntax

```
show running-config interface IFNAME ip multicast
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip multicast
!
interface eth1
!
```

show running-config prefix-list

Use this command to display the running system status and configuration details for prefix lists.

Command Syntax

```
show running-config prefix-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config prefix-list
!
ip prefix-list abc seq 5 permit any
ip prefix-list as description annai
ip prefix-list wer seq 45 permit any
!
```

show running-config vrf

Use this command to show the running system status and configuration details for a specified VRF instance name.

Command Syntax

```
show running-config vrf WORD
```

Parameters

WORD	Virtual Routing and Forwarding name

Command Mode

Privileged exec mode, configure mode, router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config vrf xyz
!
ip vrf xyz
 description vrf
 router-id 11.11.11.11
```

show tcp

Use this command to display the Transmission Control Protocol (TCP) connections details.

Command Syntax

```
show tcp
```

Parameters

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tcp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*              LISTEN
tcp        0      1 10.12.44.1:57740      127.0.0.1:705          CLOSE_WAIT
tcp       52      0 10.12.44.21:22        10.12.7.89:705         ESTABLISHED
tcp       85      0 10.12.44.21:57742     10.12.44.21:57738      ESTABLISHED
```

Table 1-31: Show tcp output

Entry	Description
Proto	Protocol – TCP
Recv-Q	Number of TCP packets in the Receive Queue.
Send-Q	Number of TCP packets in the Send-Q.
Local Address and port number	Local IP address and the port number.

Table 1-31: Show tcp output (Continued)

Entry	Description
Foreign Address and port number	Foreign (received) IP address and the port number.
State	Current state of TCP connections: ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2 TIME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING UNKNOWN

show users

Use this command to display information about current users.

Command Syntax

```
show users
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

      Line      User     Idle     Location/Session      PID     TYPE        Role
(*) 130 vty 0 [C]root   00:00:36      pts/0            20872    Local    network-admin
(#)   NA      [N]root     NA           1                 NA      NA      network-admin
      NA      [N]root     NA           2                 NA      NA      network-admin
    131 vty 1 [C]joyce  00:00:26     pts/1             17593    Remote   network-admin
```

Table 1-32 explains the output fields.

Table 1-32: show users fields

Entry	Description
Current users	
CLI user	
Location	
Session	
Lock acquired by user	
Netconf users	
Line	
User	User name.

Table 1-32: show users fields

Entry	Description
Idle	How long the user has been idle.
Location/Session	
PID	Process identifier name.
Type	
Role	

terminal width

Use this command to set the number of characters to be displayed in one line on the screen. Use the no option to unset the number of characters on the screen.

Note: If user wants to have a fixed terminal length and width, then terminal length should not be set to 0. i.e. CLI “terminal length 0“ should not be used, and only non-zero length to be used.

Command Syntax

```
terminal width <24-511>
terminal no width <24-511>
```

Parameters

<24-511>	Number of lines on screen

Default

Default width value 80 is optionally overridden by kernel.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
host#terminal width 120
```

terminal length

Use this command to set the number of lines displayed on the screen.

Use the no option to unset the number of lines on a screen.

Note: If user wants to have a fixed terminal length and width, then terminal length should not be set to 0. i.e. CLI “terminal length 0“ should not be used, and only non-zero length to be used.

Command Syntax

```
terminal length <0-511>
terminal no length <0-511>
```

Parameters

<0-511>	Number of lines on screen. Specify 0 for no pausing.

Default

Default length value 24 is optionally overridden by kernel.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#terminal length 0
```

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

terminal monitor

Use this command to display debugging output on a terminal.

Use one of the optional parameters to display debugging output for the OcNOS user. When the command is used without a parameter, it can be used by a OcNOS user to display the debug output on the terminal for the user local OcNOS. When used with a parameter, it may be used only by a OcNOS user.

The no form of the command terminates the debug output on the terminal. The OcNOS user can use this command. In addition, the OcNOS user can cancel a debug output from a specific VR or all VRs.

Command Syntax

```
terminal monitor
terminal monitor (all|WORD|)
terminal no monitor
terminal no monitor (WORD|)
```

Parameters

`WORD`	Used in the PVR context, and contains the VR name to be included in the debugging session.
`all`	Used the PVR context to include all VR in a PVR debugging session.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>Enable
#terminal monitor
#terminal no monitor
```

write

Use this command to a write the configuration to the file used at startup or to a specified file. This is the same as the copy running-config startup-config command.

Command Syntax

```
write file FILE
write memory
write WORD
```

Parameters

`FILE`	Write to a given path and file. If you do not give a file path, the file is added to `/root`.
`memory`	Write to non-volatile memory.
`WORD`	Write to running configuration file path.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows writing the configuration to the startup configuration file:

```
#write
Building configuration...
[OK]
```

This example shows writing the configuration to a specified file:

```
#write file /home/test.txt
Building configuration...
[OK]
```

CHAPTER 2 IMI Shell Commands

This chapter describes IMI shell commands.

do

Use this command to run several exec mode or privileged exec mode commands from configure mode. The commands that can be run from configure mode using `do` are: `show`, `clear`, `debug`, `ping`, `traceroute`, `write`, and `no debug`.

Command Syntax

```
do LINE
```

Parameters

`LINE`	Command and its parameters.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#(config)#do show interface
Interface lo
  Hardware is Loopback index 1 metric 1 mtu 16436 duplex-half arp ageing
timeout 25
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet 4.4.4.40/32 secondary
  inet 127.0.0.1/8
  inet6 ::1/128
  Interface Gifindex: 3
  Number of Data Links: 0
  GMPLS Switching Capability Type:
    Packet-Switch Capable-1 (PSC-1)
  GMPLS Encoding Type: Packet
  Minimum LSP Bandwidth 0
    input packets 10026, bytes 730660, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 10026, bytes 730660, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
#
```

logout

Use this command to exit the OcNOS shell.

Command Syntax

```
logout
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>logout
[root@TSUP40 sbin]#
```

ping

Use this command to send echo messages to another host.

Command Syntax

```
ping WORD (vrf (NAME|management)|)
ping ip WORD (vrf (NAME|management)|)
ping ipv6 WORD (|IFNAME)
ping ipv6 WORD (|IFNAME) (vrf (NAME|management)|)
```

Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.
IFNAME	Name of the interface.

Default

No default value is specified

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping 20.20.20.1 vrf management
Press CTRL+C to exit
PING 20.20.20.1 (20.20.20.1) 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=64 time=0.036 ms

--- 20.20.20.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

```
rtt min/avg/max/mdev = 0.032/0.034/0.036/0.006 ms

#ping ipv6 3001:db8:0:1::129 vrf management
Press CTRL+C to exit
PING 3001:db8:0:1::129(3001:db8:0:1::129) 56 data bytes
64 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=8 ttl=64 time=0.048 ms

--- 3001:db8:0:1::129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

interactive ping

Use this command to send echo messages to another host interactively. You are prompted with options supported by the command.

Command Syntax

```
ping
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping
Protocol [ip]:
Target IP address: 20.20.20.1
Name of the VRF : management
Repeat count [5]: 6
Time Interval in Sec [1]: 2.2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Ping Broadcast? Then -b [n]:
PING 20.20.20.1 (20.20.20.1) 100(128) bytes of data.
108 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.037 ms
108 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.034 ms

--- 20.20.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11000ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.007 ms

#ping
Protocol [ip]: ipv6
Target IP address: 3001:db8:0:1::129
Name of the VRF : management
Repeat count [5]:
Time Interval in Sec [1]:
Datagram size [100]:
```

```
Timeout in seconds [2]:
Extended commands [n]:
PING 3001:db8:0:1::129(3001:db8:0:1::129) 100 data bytes
108 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.050 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.042 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.048 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.051 ms

--- 3001:db8:0:1::129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.042/0.047/0.051/0.008 ms
```

The input prompts are described in Table 2-33:

Table 2-33: ping output fields

Protocol [ip]	IPv4 or IPv6. The default is IPv4 if not specified.
Target IP address	IPv4 or IPv6 address or host name.
Name of the VRF	Name of the Virtual Routing and Forwarding instance.
Repeat count [5]	Number of ping packets to send. The default is 5 if not specified.
Time Interval in Sec [1]	Time interval between two ping packets. The default is 1 second if not specified.
Datagram size [100]	Ping packet size. The default is 100 bytes if not specified.
Timeout in seconds [2]	Time to wait for ping reply. The default is 2 seconds if not specified.
Extended commands [n]	Options for extended ping. The default is “no”.
Source address or interface	Source address or interface.
Type of service [0]	Types of service. The default is 0 if not specified.
Set DF bit in IP header? [no]	Do not fragment bit. The default value is “no” if not specified.
Data pattern [0xABCD]	Specify a pattern.
Ping Broadcast? Then -b [n]	Broadcast ping. The default is “no”. For a broadcast address, the value should be “y”.

privilege level

Use this command to set the command privilege level.

Note: Privilege levels 2-14 are undefined.

Use the no parameter with this command to disable the command privilege level.

Command Syntax

```
privilege level <1-15>
privilege level (16)
no privilege level (<1-15>|)
no privilege level (16)
```

Parameters

16	Maximum privilege level for a line.
<1-15>	Default privilege level for a line.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#line vty 0 5
(config-line)#privilege level 15
```

show privilege

Use this command to display the current privilege level. The privilege level range is 1-15.

Command Syntax

```
show privilege
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show privilege
Current privilege level is 15
#
```

telnet

Use this command to open a telnet session.

Command Syntax

```
telnet WORD vrf management|)
telnet WORD PORT
```

Parameters

WORD	IP address or hostname of a remote system.
PORT	TCP port number.
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#telnet 2.2.2.2 2602
trying telnet 2.2.2.2 2602...
```

traceroute

Use this command to trace an IPv4/v6 route to its destination.

Command Syntax

```
traceroute WORD
traceroute WORD (vrf (NAME|management)|)
traceroute ip WORD
traceroute ip WORD (vrf (NAME|management)|)
traceroute ipv6 WORD
traceroute ipv6 WORD (vrf (NAME|management)|)
```

Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#traceroute ip 10.10.100.126 vrf management
traceroute to 10.10.100.126 (10.10.100.126), 30 hops max, 38 byte packets
 1  10.1.2.1 (10.1.2.1)  0.386 ms  0.315 ms  0.293 ms
 2  10.10.100.126 (10.10.100.126)  1.944 ms  1.497 ms  1.296 ms
#
```

write terminal

Use this command to display the current configuration.

Command Syntax

```
write terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#write terminal

Current configuration:
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
 redistribute connected
!
line vty
 exec-timeout 0 0
```

CHAPTER 3 VLOG Commands

This chapter describes virtual router log (VLOG) commands.

show vlog all

Use this command to display the output of all virtual router log `show` commands. For column descriptions, refer to descriptions of the individual commands.

Command Syntax

```
show vlog all
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog all

Type     Name     FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8  12  vr222    ---        1
tty   /dev/pts/4  13  <PVR>    ---        1

VR-Name  VR-Id  PVR-Terms  VR-Terms                  LogFile
CurSize
<PVR>       0          1        0         /var/local/zebos/log/pvr/my-log
1624320
vr111       1          0        0         n/a
n/a
vr222        2          0        1          /var/local/zebos/log/vr222/log-
vr222        0
vr333        3          0        0          /var/local/zebos/log/vr333/log-
vr333        0

Name  Id  MsgCnt        ConTime              ReadTime
NSM    1       1  Fri May-15 21:05:04  Fri May-15 21:05:04
IMI   19       1  Fri May-15 21:05:02  Fri May-15 21:05:02
```

Table 3-34 explains the output:

Table 3-34: show vlog all details

Name	Name of protocol module
Id	Protocol module identifier

Table 3-34: show vlog all details

MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

Table 3-35 explains the output:

Table 3-35: show vlog all details

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

Table 3-36 explains the output:

Table 3-36: show vlog all details

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

show vlog clients

Use this command to display all attached virtual router log clients (protocol modules).

Command Syntax

```
show vlog clients
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog clients

Name  Id  MsgCnt          ConTime               ReadTime
NSM    1       1     Fri May-15 21:05:04  Fri May-15 21:05:04
IMI   19       1     Fri May-15 21:05:02  Fri May-15 21:05:02
```

Table 3-37 explains the output:

Table 3-37: show vlog clients details

Name	Name of protocol module
Id	Protocol module identifier
MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

show vlog terminals

Use this command to display all active connections where VLOGD is forwarding log output.

Command Syntax

```
show vlog terminals
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog terminals

Type     Name     FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8  12  vr222    ---        1
tty   /dev/pts/4  13  <PVR>    ---        1
```

Table 3-38 explains the output:

Table 3-38: show virtual router log terminals details

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

show vlog virtual-routers

Use this command to display virtual router statistics such as the number of terminals attached.

Command Syntax

```
show vlog virtual-routers
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog virtual-routers

VR-Name  VR-Id  PVR-Terms  VR-Terms LogFile
CurSize
<PVR>         0  1          0        /var/local/zebos/log/pvr/my-log
1624320
vr111         1  0          0        n/a                                    n/a
vr222         2  0          1        /var/local/zebos/log/vr222/log-vr222  0
vr333         3  0          0        /var/local/zebos/log/vr333/log-vr333  0
```

Table 3-39 explains the output:

Table 3-39: show vlog virtual-routers details

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

CHAPTER 4 System Commands

This chapter is a reference for system commands.

mv

Use this command to rename (move) a file.

Command Syntax

```
mv LINE
```

Parameters

LINE	Source and destination file names

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#mv old-name new-name
```

pwd

Use this command to print the working directory.

Command Syntax

pwd

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

#pwd

CHAPTER 5 Licensing and Upgrade Commands

This chapter describes the license and upgrade commands.

license get

Use this command to fetch the license for this device from a network path or a USB mount path. This command validates the license against the device identifier.

Note: The system date must be correct to avoid installation failure.

For HTTP, FTP, or TFTP, ensure that the IP address is reachable from the OcNOS device and that the file location is correct.

If you install a license from a USB stick, insert it, and the contents of the USB are available as `///mnt/usb/`. For example:

```
>license get file:///mnt/usb/IPI-CC37ABBE0340.bin
```

After running the `license get` command, you can immediately use the switch without rebooting.

To verify, run the show license command after giving this command.

Command Syntax

```
license get (|(source-interface IFNAME)) WORD
```

Parameters

`IFNAME`	The interface used to download the license. If not specified, `eth0` is used. If the management interface of the switch is in the “management” VRF, then this command uses the “management” VRF to get the license from the specified path. You do need not to know if the management port is in the default VRF or the “management” VRF.

`WORD`	Where to get the license:
	`ftp://your-server-ip/path/to/file/IPI_deviceId.bin`
	`http://your-server-ip/path/to/file/IPI_deviceId.bin`
	`tftp://your-server-ip/path/to/file/IPI_deviceId.bin`
	`file:///mnt-point/usb/path/to/file/IPI_deviceId.bin`

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>license get http://myServer/IPI-CC37ABBE0340.bin
```

Specify the `source-interface` parameter to set the interface to use:

```
>license get source-interface xe2 http://myServer/IPI-CC37ABBE0340.bin
```

license refresh

Use this command to install a license present on the device. This command is required only when the license get command reports error when installing the license but successfully downloaded the license.

When this command is given without a file name, the device installs the most recently downloaded license file.

Note: Always ensure that the device date is up to date to avoid license installation failures.

Once this command is successful, you can use the device without rebooting. Verify license installation with the show license command.

Command Syntax

```
license refresh (FILENAME|)
```

Parameters

FILENAME	License file name which exists on the device.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Examples

```
>license refresh
>license refresh IPI-CH3QX42.bin
```

show installers

Use this command to display a list of downloaded images on the device.

Command Syntax

```
show installers
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#show installers
/installers/DELL_S6000_ON-OcNOS-1.3.6.228a-DC_MPLS-S0-P0-installer
#
```

show license

Use this command to display the current license details and errors. The licenses are device locked, which means that a separate license is required for each device.

Command Syntax

```
show license
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>show license
License Type: Trial edition
Remaining day to expires : 21 day(s)
Node Identifier: 1402EC2DA140
Device Software : OCNOS-ENT-IPBASE

>show license
License Type: Evaluation, Limited edition
License Validity: Not Applicable
Node Identifier: A82BB59DCAD9
Device Software : OCNOS-DC-IPBASE
License Error: Invalid license file
```

show sys-update details

Use this command to display upgrade details. The output indicates whether the current version is committed or rolled back.

Command Syntax

```
show sys-update details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show sys-update details
Previous_version EC_AS5812_54X-OcNOS-1.3.4.265-DC_MPLS_ZEBM-S0-P0
Current_version EC_AS5812_54X-OcNOS-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer
(committed)
Last_upgraded Wed Sep 26 14:40:06 UTC 2018
Auto Rollback end time NA
```

sys-update commit

Use this command to accept a new version. After a commit, you cannot roll back to a previous version. Until you commit a new version, you cannot save the configuration. Upgrading with an installer file is auto committed.

Command Syntax

```
sys-update commit
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update commit
```

sys-update delete

Use this command to delete a downloaded image.

Command Syntax

```
sys-update delete IMAGE_NAME
```

Parameters

IMAGE_NAME	Installer to delete

Default

None

Command mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#sys-update delete DELL_S6000_ON-OcNOS-1.3.6.228a-DC_MPLS-S0-P0-installer
```

sys-update get

Use this command to download an installer image.

Note: The URL must be compliant with RFC 3986.

Note: At times while downloading installer through TFTP protocol, download progress would show 100% from the start to the end of the download. This behavior is observed whenever the TFTP server doesn't support the TFTP Option Negotiation. Also at times TFTP download takes more time to download the installer though the client and server are part of the same subnet, eventually download operation even times out after 30 minutes. The reason for such issue is the latency, here some of the TFTP server implementations are lagging performance. In such instances we recommend to switch to a different TFTP server. This TFTP download operation is verified in Debian Linux machine against the server present in the `tftpd-hpa` package.

Command Syntax

```
sys-update get ((source-interface IFNAME)|) URL (verbose|)
```

Parameters

`IFNAME`	The interface used to download the new version. If not specified, eth0 is used.

`URL`	Where to get the installer:
	`http://your-server-ip/path/to/file/<abc-installer>`
	`ftp://your-server-ip/path/to/file/<abc-installer>`
	`tftp://your-server-ip/path/to/file/<abc-installer>`
	`file:///mnt/usb/path/to/file/<abc-installer>`

`verbose`	Include download logs in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#sys-update get source-interface xe3 http://myServer/EC_AS5812_54X-OcNOS-1.3.7.52-
DC_IPBASE-S0-P0-installer
```

sys-update install

Use this command to upgrade the current software to a newer version. You can do two types of installation:

- If a `.deb` file is provided, the board is loaded with new binaries.
- If an installer file is provided, the board is completely installed with a new kernel and binaries.

Note:

1. During an upgrade, if a license is not available the existing configuration is not applied. Also, the `ZebOS.conf` file is not created and the terminal monitor command is not allowed.
2. The URL must be compliant with RFC 3986.
3. When this command is executed without the `source-interface` parameter, then eth0 and the default management VRF are used. When this command is executed with the `source-interface` parameter then that interface is used.
4. At times while downloading installer through TFTP protocol, download progress would show 100% from the start to the end of the download. This behavior is observed whenever the TFTP server doesn't support the TFTP Option Negotiation. Also at times TFTP download takes more time to download the installer though the client and server are part of the same subnet, eventually download operation even times out after 30 minutes. The reason for such issue is the latency, here some of the TFTP server implementations are lagging performance. In such instances we recommend to switch to a different TFTP server. This TFTP download operation is verified in Debian Linux machine against the server present in the `tftpd-hpa` package.

Command Syntax

```
sys-update install (|(source-interface IFNAME)) URL (verbose|)
```

Parameters

`IFNAME`	The interface used to download the new version. If not specified, `eth0` is used.

`URL`	Where to get the new version:
	`http://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`ftp://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`tftp://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`file:///mnt/usb/path/to/file/<abc-updater.deb or abc-installer>`

`verbose`	Include upgrade logs in the output.

Default

None

Caution

OcNOS services are using `/usr/local/etc` path to store the device configuration, and this path mounted into a separate partition to isolate system configurations. This partition is meant only for system configuration. It will affect the system stability if the user uses this partition for storing general files. In this problematic state, if the device reboots, OcNOS services will not start properly, that would even create problems to the device connectivity. There will be an impact on normal system configuration operations.

User must take care of this problem just before issuing the following commands:

- `reload/sys-reload` - Reboots the device.
- `sys-shutdown` - This is to shutdown the device, but when users powers the device OcNOS services won't start cleanly.
- `reboot / shutdown` - From Linux shell
- Also includes all copy commands from Linux shell before issuing the user triggered reload commands.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update install source-interface eth2 http://10.12.52.150/myServer/
EC_AS5812_54X-OcNOS-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-updater.deb
```

sys-update list-version

Use this command to display files and folders. This command supports only FTP and the local file system.

Command Syntax

```
sys-update list-version ((source-interface IFNAME)|) URL
```

Parameters

`IFNAME`	The interface used to download the list. If not specified, `eth0` is used.

`URL`	Where to get the list:
	`ftp://(username@|)serverIP/path/to/file/`
	`file:///mnt/usb/path/to/file/`

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update list-version ftp://10.12.52.150/
```

sys-update rollback

Use this command to roll back to the previous version. After a commit, you cannot roll back. Upgrading with an installer file does not support roll back.

Command Syntax

```
sys-update rollback (verbose|)
```

Parameters

verbose	Include details in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update rollback
#sys-update rollback verbose
```

sys-update un-install

Use this command to un-install the device software remotely using the CLI and NetConf.management interfaces. This command decouples the device console dependency to un-install OcNOS.

This command puts the device in ONIE un-install mode and triggers device reboot. Upon reboot, ONIE detects the un-install mode and performs the un-installation. Once the un-installation completes, the device boots ONIE. To understand more about the un-installation technique, see the U-Boot and x86 Architecture sections at:

https://opencomputeproject.github.io/onie/design-spec/index.html#.

Note: By default, ONIE has SSH and Telnet services running, so you also have the option to trigger the installation through the management connection. For more information about SSH and Telnet connectivity, see:

https://opencomputeproject.github.io/onie/user-guide/index.html#debugging-an-installation.

Command Syntax

```
sys-update un-install
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#sys-update un-install
```

Network Services Module Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Common Exec Mode Commands

This chapter is a reference for Exec and Privileged mode commands. All commands are common to multipleprotocols. This chapter includes the following commands:

clear interface fec

Use this command to clear FEC (forward error correction) statistics on a specified interface or on all interfaces.

Note: This command is not supported on loop-back interfaces or the out-of-band (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface ce1/1 fec
```

copy empty-config startup-config

Use this command to clear the contents of the startup configuration.

Command Syntax

```
copy empty-config startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy empty-config startup-config
#
```

debug nsm all

Use this command to enable NSM debugging.

Use the no parameter with this command or the undebug command to disable NSM debugging.

Command Syntax

```
debug nsm (all|)
no debug nsm (all|)
undebug nsm (all|)
```

Parameters

all	Enable all debugging.

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug nsm all
#
```

debug nsm bfd

Use this command to enable debugging BFD (Bidirectional Forwarding Detection) events.

Use the no parameter with this command or the undebug command to disable BFD debugging.

Command Syntax

```
debug nsm bfd
no debug nsm bfd
undebug nsm bfd
```

Parameters

None

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug nsm bfd
#
```

debug nsm events

Use this command to enable debugging of NSM events.

Use the no parameter with this command or the undebug command to disable event debugging.

Command Syntax

```
debug nsm events
no debug nsm events
undebug nsm events
```

Parameters

None

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug nsm events
#
```

debug nsm hal

Use this command to enable debugging of NSM HAL (hardware abstraction layer) events.

Use the no parameter with this command or the undebug command to disable HAL debugging.

Command Syntax

```
debug nsm hal (all|) debug
debug nsm hal events
no debug nsm hal (all|)
no debug nsm hal events
undebug nsm hal events
```

Parameters

all	Enable all HAL debugging.
events	Enable debugging of only NSM HAL events.

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug nsm hal all
#
```

debug nsm mpls

Use this command to enable MPLS NSM logs.

Use the no parameter with this command or the undebug command to disable MPLS NSM logs.

Command Syntax

```
debug nsm mpls
no debug nsm mpls
```

Parameters

None

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS-SP version 3.1.

Example

```
#debug nsm mpls
#
```

debug nsm packet

Use this command to enable debugging of NSM packet events.

Use the no parameter with this command or the undebug command to disable packet debugging.

Command Syntax

```
debug nsm packet (recv|send|) (detail|)
no debug nsm packet (recv|send|) (detail|)
undebug nsm packet (recv|send|) (detail|)
```

Parameters

recv	Specify the debug option-set for receive packet.
send	Specify the debug option-set for send packet.
detail	Sets the debug option to provide detailed information.

Default

By default, debug command is disabled.

Command Mode

Privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug nsm packet
#debug nsm packet recv detail
#
```

reload

Use this command to shut down the device and perform a cold restart. You call this command when:

- You detect a configuration issue such as `show running-config` displaying a configuration but when you try to remove that configuration, you get a message that it is not configured.
- You have replaced the start-up configuration file (in this case you specify the `flush-db` parameter).

Command Syntax

```
reload (flush-db|)
```

Parameters

`flush-db`	Delete the database file and recreate it from the start-up configuration file.

Default

No default value is specified

Caution

OcNOS services are using `/usr/local/etc` path to store the device configuration, and this path mounted into a separate partition to isolate system configurations. This partition is meant only for system configuration. It will affect the system stability if the user uses this partition for storing general files. In this problematic state, if the device reboots, OcNOS services will not start properly, that would even create problems to the device connectivity. There will be an impact on normal system configuration operations.

User must take care of this problem just before issuing the following commands:

- `sys-reload` - Reboots the device.
- `sys-update` - Device reboots after upgrading the NOS software.
- `sys-shutdown` - This is to shutdown the device, but when users powers the device OcNOS services won't start cleanly.
- `reboot / shutdown` - From Linux shell
- Also includes all copy commands from Linux shell before issuing the user triggered reload commands.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows replacing a start-up configuration file and then synchronizing it to the configuration database:

```
#copy file /home/TEST.conf startup-config
Copy Success
#
#reload flush-db
The system has unsaved changes.
Would you like to save them now? (y/n): n
```

```
Configuration Not Saved!
Are you sure you would like to reset the system? (y/n): y
```

For both of these prompts, you must specify whether to save or discard the changes. Abnormal termination of the session without these inputs can impact the system behavior.

For the `unsaved changes` prompt:

`Would you like to save them now?`

You should always say “no” to this prompt because otherwise the command takes the current *running configuration* and applies it to the current start-up configuration.

show cli

Use this command to display the command tree of the current mode.

Command Syntax

```
show cli
```

Parameters

None

Default

None

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
        +-domain
          +-DOMAIN_NAME [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
        +-level
          +-LEVEL_ID [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
      +-maintenance-points
        +-remote
          +-domain
            +-DOMAIN_NAME [clear ethernet cfm maintenance-points remote(domain
D
--More--
```

show debugging nsm

Use this command to display debugging information.

Command Syntax

```
show debugging nsm
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
#
```

show interface fec

Use this command to display the FEC (forward error correction) statistics for an interface.

Note: You can only display FEC statistics for physical interfaces and not for management or logical interfaces.

Command Syntax

```
show interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface ce1/1 fec

+----------------+--------+-----------------------------------------------+
|  Interface  | FEC  | CORRECTED BLOCK COUNT | UNCORRECTED BLOCK COUNT |
+----------------+--------+-----------------------------------------------+
   ce1/1         off         0                           0
```

Table 1-40 explain the fields in the command output.

Table 1-40: show interface fec

Field	Description
Interface	Name of the configured interface.
FEC	Status of the forwarding equivalence class.
Corrected Block Count	Number of the corrected block count.
Uncorrected Block Count	Number of the uncorrected block count.

show ip rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax

```
show ip rpf A.B.C.D
show ip rpf (vrf NAME|) A.B.C.D
```

Parameters

A.B.C.D	IP address of multicast source.
NAME	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip rpf 10.10.10.50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

show ipv6 rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax

```
show ipv6 rpf X:X::X:X
show ipv6 rpf (vrf NAME|) X:X::X:X
```

Parameters

X:X::X:X	IP address of multicast source.
NAME	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 rpf 10:10::10:50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

Table 1-41 explains the output fields.

Table 1-41: show ipv6 rpf output fields

Field	Description
RPF Interface	Name of the RPF interface.
RPF neighbor	Upstream RPF neighbor.
RPF route	Route table in which the logical interface address is located.
RPF type	Different type of RPF like multicast, unicast, MBGP, DVMRP, or static mroutes.

Table 1-41: show ipv6 rpf output fields

Field	Description
RPF recursion count	Number of times that the router lookups its routing table more than once to find out the immediate next-hop and exiting interface.
Distance	IPv6 address of the remote side of the connection. Doing distance-preferred lookups across tables.
Metric	Metrics are informational units that can be measured and compared.

show list

Use this command to display the commands relevant to the current mode.

Command Syntax

```
show list
```

Parameters

None

Default

None

Command Mode

All command modes except IPv4 access-list and IPv6 access-list mode.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>show list
 clear arp-cache
  clear bgp *
  clear bgp * in
  clear bgp * in prefix-filter
  clear bgp * out
  clear bgp * soft
  clear bgp * soft in
  clear bgp * soft out
  clear bgp <1-4294967295>
  clear bgp <1-4294967295> in
  clear bgp <1-4294967295> in prefix-filter
  clear bgp <1-4294967295> out
  clear bgp <1-4294967295> soft
  clear bgp <1-4294967295> soft in
  clear bgp <1-4294967295> soft out
  clear bgp (A.B.C.D|X:X::X:X)
  clear bgp (A.B.C.D|X:X::X:X) in
  clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
  clear bgp (A.B.C.D|X:X::X:X) out
  clear bgp (A.B.C.D|X:X::X:X) soft
  clear bgp (A.B.C.D|X:X::X:X) soft in
  clear bgp X:X::X:X soft out

--more--
```

show nsm client

Use this command to display NSM client information including the services requested by the protocols, statistics and the connection time

Command Syntax

```
show nsm client
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
 IMI, socket 23
  Service: Interface Service, Router ID Service, VRF Service
  Messsage received 1, sent 58
  Connection time: Thu Jul 22 11:03:12 2010
  Last message read: Service Request
  Last message write: Link Up
NSM client ID: 25
 ONMD, socket 24
  Service: Interface Service, Bridge service, VLAN service
  Messsage received 2, sent 74
  Connection time: Thu Jul 22 11:03:15 2010
  Last message read: OAM  LLDP msg
  Last message write: Link Up
#
```

show process

Use this command to display a process ID, the name of the process, how long the process has been running and any faults detected on the process.

Command Syntax

```
show process
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show process
 PID NAME             TIME FD
   1 nsm          01:49:24 6

#
```

Table 1-42 explains the output fields.

Table 1-42: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S): Number of system and user CPU seconds that the process has used. (None, D, and E): Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.

show running-config router

Use this command to display the running system router configuration.

Command Syntax

```
show running-config router bgp
show running-config router isis
show running-config router ldp
show running-config router ospf
show running-config router rip
show running-config router rsvp
show running-config router vrrp
```

Parameters

`bgp`	Display Border Gateway Protocol (BGP) information.
`isis`	Display Intermediate System to Intermediate System (IS-IS) information.
`ldp`	Display Label Distribution Protocol (LDP) information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`rsvp`	Display Resource Reservation Protocol (RSVP) information.
`vrrp`	Display Virtual Router Redundancy Protocol (VRRP) information.

Default

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config router vrrp
!
router-id 3.3.3.3
!
```

show running-config switch

Use this command to display the running system switch configuration.

Command Syntax

```
show running-config switch bridge
show running-config switch gmrp
show running-config switch gvrp
show running-config switch lacp
show running-config switch lmi
show running-config switch mstp
show running-config switch radius-server
show running-config switch rpsvt+
show running-config switch rstp
show running-config switch ptp
show running-config switch stp
show running-config switch synce
show running-config switch vlan
```

Parameters

`bridge`	Display Bridge group information.
`gmrp`	Display GARP Multicast Registration Protocol (GMRP) information.
`gvrp`	Display GARP VLAN Registration Protocol (GVRP) information.
`lacp`	Display Link Aggregation Control Protocol (LACP) information.
`lmi`	Display Ethernet Local Management Interface Protocol (LMI) information.
`mstp`	Display Multiple Spanning Tree Protocol (MSTP) information.
`radius-server`	Display RADIUS server information.
`rpvst+`	Display Rapid Per-VLAN Spanning Tree (rpvst+) information.
`rstp`	Display Rapid Spanning Tree Protocol (RSTP) information.
`ptp`	Display Precision time Protocol (PTP)
`stp`	Display Spanning Tree Protocol (STP) information.
`synce`	Display synce information.
`vlan`	Display values associated with a single VLAN.

Default

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config switch stp
!
bridge 6 ageing-time 45
bridge 6 priority 4096
bridge 6 max-age 7
```

show running-config urpf

Use this command to check uRPF status for this system.

Command Syntax

```
show running-config urpf
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config urpf
ip urpf enable

(config)#show running-config urpf
ip urpf enable
```

show startup-config

Use this command to display the startup configuration.

Command Syntax

```
show startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show startup-config
!   2001/04/21 11:38:52
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```

show version

Use this command to display OcNOS version information.

Command Syntax

```
show version
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show version
Software version: EC_AS5812-54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0 09/27/2018
13:44:22
 Copyright (C) 2018 Coriant. All rights reserved

 Software Product: OcNOS, Version: 1.3.4.268
 Hardware Model: Edgecore 5812-54X-O-AC-F
 Software Feature Code: DC-MPLS-ZEBM
 System Configuration Code: S0
 Package Configuration Code: P0
 Software Baseline Version: 1.3.4.208

Installation Information:
 Image Filename: EC_AS5812_54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0-installer
 Install method: http
 ONIE SysInfo: x86_64-accton_as5812_54x-r0
#
```

Table 1-43: Show version output

Entry	Description
Software version	The software version including hardware device name and date.
Software Product	Product name and version.
Hardware Model	Hardware platform.
Software Feature Code	SKU that specifies the capabilities of this version of the software.
System Configuration Code	System configuration number.

Table 1-43: Show version output (Continued)

Entry	Description
Package Configuration Code	ONIE package installer versions.
Software Baseline Version	Version from which this release branch is created.
Installation Information	Information about the installation.
Image Filename	The file name of the installed image.
Install method	The type of server (or USB stick) from which the software was installed.
ONIE SysInfo	ONIE version.

sys-reload

Use this command to cold restart the device.

Note: This command is an alias for the reload command.

Command Syntax

```
sys-reload
```

Parameters

None

Default

None

Caution

OcNOS services are using `/usr/local/etc` path to store the device configuration, and this path mounted into a separate partition to isolate system configurations. This partition is meant only for system configuration. It will affect the system stability if the user uses this partition for storing general files. In this problematic state, if the device reboots, OcNOS services will not start properly, that would even create problems to the device connectivity. There will be an impact on normal system configuration operations.

User must take care of this problem just before issuing the following commands:

- `reload` - Reboots the device.
- `sys-update` - Device reboots after upgrading the NOS software.
- `sys-shutdown` - This is to shutdown the device, but when users powers the device OcNOS services won't start cleanly.
- `reboot / shutdown` - From Linux shell
- Also includes all copy commands from Linux shell before issuing the user triggered reload commands.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
>sys-reload
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to reset the system? (y/n): n
```

sys-shutdown

Use this command to shut down the device gracefully. After giving this command, you can remove the device power cable.

Note: Some of the switch hardwares doesn't support system shutdown. On such devices this command will make the switch to go for a reboot.

Command Syntax

```
sys-shutdown
```

Parameters

None

Default

None

Caution

OcNOS services are using `/usr/local/etc` path to store the device configuration, and this path mounted into a separate partition to isolate system configurations. This partition is meant only for system configuration. It will affect the system stability if the user uses this partition for storing general files. In this problematic state, if the device reboots, OcNOS services will not start properly, that would even create problems to the device connectivity. There will be an impact on normal system configuration operations.

User must take care of this problem just before issuing the following commands:

- `reload/sys-reload` - Reboots the device.
- `sys-update` - Device reboots after upgrading the NOS software.
- `reboot / shutdown` - From Linux shell
- Also includes all copy commands from Linux shell before issuing the user triggered reload commands.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
>sys-shutdown
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to shutdown the system? (y/n): y
For both of these prompts, you must specify whether to save or discard the
changes.
For the unsaved changes prompt:
Would you like to save them now?
```

CHAPTER 2 Common Configure Mode Commands

This chapter provides a reference for the configure mode commands.

automatic-router-id-selection enable

Use this command to assure that OcNOS selects the loopback IP address as the router-id each time the device is rebooted.

Use the no form of this command to remove this constraint.

Command Syntax

```
automatic-router-id-selection enable
no automatic-router-id-selection enable
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#automatic-router-id-selection enable
```

clear router-id

Use this command to clear the current Router-Id and trigger the Router-Id calculation again. The new Router-id is sent to all protocol modules.

- To clear only the router-id for the default VRF, enter `clear router-id`.
- To clear the router-id for a particular VRF, enter `clear router-id vrf VRFNAME`.
- To clear the router-id for all VRFs, enter `clear router-id vrf`.

Note: If router-id is not configured, highest ip address configured on the interface is chosen as router-id. if chosen ip address is unconfigured, make sure to execute clear router-id before configuring a new router-id.

Command Syntax

```
clear router-id (vrf (VRFNAME|))
```

Parameters

VRFNAME	VPN routing/forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#clear router-id
(config)#


#configure terminal
(config)#clear router-id vrf
(config)#
```

clock timezone

Use this command to set the system time zone.

Use no form of this command to set the default system time zone (UTC).

Command Syntax

```
clock timezone (WORD)
no clock timezone
```

Parameters

WORD	Timezone name. Use 'show timezone' to get the list of city names.

Default

By default, system time zone is UTC

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#clock timezone Los_Angeles
```

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: When mac-move-limit ErrDisable is enabled globally, then all interfaces are enabled. mac-move-limit ErrDisable can be enabled globally, but disabled for a specific interface with the `no mac-move-limit errdisable` command.

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax

```
errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap| mac-move-limit  }
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap | mac-move-limit  }
```

Parameters

`stp-bpdu-guard`	ErrDisable on stp-bpdu-guard
`lag-mismatch`	ErrDisable on lag-mismatch
`link-flap`	ErrDisable on link-flap
`mac-move-limit`	Enable or Disable Mac-Move-Limit

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax

```
errdisable link-flap-setting max-flaps <1-100> time <1-1800>
```

Parameters

<1-100>	Maximum flap count
<1-1800>	Sliding window size in seconds

Default

Five flaps in ten seconds:

Maximum flap count: 5

Sliding window size: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable mac-move-limit

Use this command to set the ErrDisable mac movement limit.

Command Syntax

```
errdisable mac-move-limit <1-1000>
```

Parameters

<1-1000>	Allowed Mac movement in 5 seconds

Default

By default, mac-move-limit is 1000

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#errdisable mac-move-limit 50
```

errdisable timeout

Use this command to set the ErrDisable auto-recovery timeout interval.

Command Syntax

```
errdisable timeout interval <10-1000000>
```

Parameters

`<10-1000000>`	Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout interval 1000
```

forwarding profile

Use this command to configure different forwarding profiles in hardware.

Note: It is required to save the configuration and reboot the board for the new forwarding profile to come into effect in the hardware.

Use show forwarding profile limit to verify the configured profile.

Command Syntax

```
forwarding profile (kaps (profile-one | profile-two)) | (elk-tcam (profile-one |
  profile-two | profile-three | custom-profile))
```

Parameters

For details about these profiles, see show forwarding profile limit.

`kaps`	Internal KBP routing table
`profile-one`	KAPS profile one
`profile-two`	KAPS profile two
`elk-tcam`	External TCAM routing table
`profile-one`	external TCAM profile one
`profile-two`	external TCAM profile two
`profile-three`	external TCAM profile three
`custom-profile`	external TCAM custom profile
`< 10-90>`	percent of ipv4 routes
`< 10-90>`	percent of ipv6 routes

Default

The default forwarding profile are as below

Table 2-44:

Is ELK-TCAM present	KAPS	ELK-TCAM
Yes	profile-two	profile-one
No	profile-one	N/A

Note:

1. elk-tcam profiles are supported only on hardware models which have external TCAM for routing.
2. forwarding profile-three is applicable on hardware model Agema AGC7648A.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version SP 1.0.

Examples

```
#configure terminal
(config)# forwarding profile elk-tcam profile-one
```

hardware-profile filter

Use this command to enable or disable TCAM filter groups. By default all filter groups will be disabled. Basic and extended groups of similar type are mutually exclusive and only one of them can be enabled at a time.

Disabling a TCAM filter group is not allowed if the group has any entries configured in hardware. Group dependent entries must be explicitly removed before disabling the TCAM group.

Note: The `qos`, `qos-ext`, and `qos-policer` filter groups can only be used for Layer 2 and IPv4 traffic. For IPv6 traffic QoS classification and actions, you must enable the `ingress-ipv6-qos` group and create an IPv6 ACL which can be matched in a class-map for applying QoS actions. For more, see Quality of Service Configuration Guide.

Note: Usually the number of extended ingress filter groups that can be created at the same time is 3. If the PIM bidirectional feature is enabled, only 2 ingress extended filter groups can be created.

For EVPN multi-homing:

- Before enabling EVPN multi-homing (evpn multi-homed command), give this command.
- Before disabling the hardware-profile, disable EVPN multi-homing.

Command Syntax

```
hardware-profile filter (ingress-l2|ingress-l2-ext|ingress-ipv4|ingress-ipv4-
ext|ingress-ipv4-qos|ingress-ipv6|ingress-ipv6-qos|qos-ipv6|ingress-arp|qos|qos-
ext|qos-policer|forwarding-ipv4|egress-l2|egress-ipv4|cfm-domain-name-str)
(enable|disable)
```

Parameter

`ingress-l2`	Ingress L2 ACL filter group.
`ingress-l2-ext`	Ingress L2 ACL, QoS, mirror filter group.
`ingress-ipv4`	Ingress IP ACL filter group.
`ingress-ipv4-ext`	Ingress IP ACL, mirror, PBR filter group.
`ingress-ipv4-qos`	Ingress IPv4 group for ACL match QoS.
`ingress-ipv6`	Ingress IPv6 ACL, mirror, PBR filter group.
`ingress-ipv6-qos`	Ingress IPv6 group for ACL match QoS.
`qos-ipv6`	Ingress QOS IPv6 group for IPv6 QoS support with statistics.
`ingress-arp`	Ingress ARP group.
`qos`	Ingress QoS filter group.
`qos-ext`	Ingress QoS extended filter group.
`qos-policer`	Ingress extended QoS group for hierarchical policer support.
`forwarding-ipv4`	Ingress IPv4 forwarding filter group.
`egress-l2`	Egress L2 ACL filter group.

`egress-ipv4`	Egress IP ACL filter group.
`cfm-domain-name-str`	Egress CFM domain group.
`enable`	Enable filter group.
`disable`	Disable filter group.

Default

By default, all filter groups are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 enable
(config)#hardware-profile filter ingress-ipv4 disable

#(config)#hardware-profile filter egress-ipv4 enable
#(config)#hardware-profile filter egress-ipv4 disable
```

Table 2-45: Table 2-56: Supported groups and the feature dependency on the groups

Group	Key Size	Security	QoS	PBR	Mirror	Statistics	
						QMX	QAX
ingress-l2	160	Yes	No	N/A	No	Yes	Yes
ingress-l2-ext	320	Yes	No	N/A	Yes	Yes	Yes
ingress-ipv4	160	Yes	No	No	No	Yes	Yes
ingress-ipv4-ext	320	Yes	No	Yes	Yes	Yes	Yes
ingress-ipv4-qos	320	N/A	Yes	N/A	N/A	Yes	Yes
ingress-ipv6	320	Yes	No	Yes	Yes	Yes	Yes
ingress-ipv6-qos	320	N/A	Yes	N/A	N/A	Yes	Yes
qos-ipv6	320	N/A	Yes	N/A	N/A	Yes	Yes
qos	160	N/A	Yes	N/A	N/A	No	No
qos-ext	320	N/A	Yes	N/A	N/A	Yes	Yes
qos-policer	320	N/A	Yes	N/A	N/A	Yes	Yes
forwarding-ipv4	80	N/A	N/A	N/A	N/A	No	No

Table 2-45: Table 2-56: Supported groups and the feature dependency on the groups

Group	Key Size	Security	QoS	PBR	Mirror	Statistics	
egress-l2	320	Yes	N/A	N/A	N/A	Yes	Yes
egress-ipv4	320	Yes	N/A	N/A	N/A	Yes	Yes
cfm-domain-name-str	160	N/A	N/A	N/A	N/A	Yes	Yes

Table 2-46: Comparison between basic and extended group qualifiers

Basic Group	Qualifiers	Extended Group	Supported qualifiers
ingress-l2	Source MAC Destination MAC Ether Type (ip, ipv6, mpls, arp, cfm, fcoe) VLAN ID Inner VLAN ID	ingress-l2-ext	Source MAC Destination MAC Ether Type VLAN ID Inner VLAN ID COS
ingress-ipv4	Source IP Destination IP IP Protocols L4 Ports	ingress-ipv4-ext	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID TCP flags
qos	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP	qos-ext	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP IP RTP L4 Ports Destination MAC Traffic type

Table 2-47: Qualifiers for other groups

Group	Qualifiers
ingress-ipv6	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 Protocols L4 Ports
forwarding-ipv4	Destination IP DSCP VRF ID

Table 2-47: Qualifiers for other groups (Continued)

Group	Qualifiers
egress-l2	Source MAC Destination MAC VLAN ID Inner VLAN ID COS
egress-ipv4	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID
qos-policer	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP IP RTP L4 Ports
ingress-ipv4-qos	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID TCP flags
ingress-ipv6-qos	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 Protocols L4 Ports
qos-ipv6	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 Protocols L4 Ports VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP
cfm-domain-name-str	MA ID

hardware-profile flowcontrol

Use this command to globally enable or disable hardware-based flow control.

Syntax

```
hardware-profile flowcontrol (disable|enable)
```

Parameters

`disable`	Disable flow control globally
`enable`	Enable flow control globally

Default

By default flow control is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#hardware-profile flowcontrol enable
```

hardware-profile service-queue

Use this command to set the number of service-queue counts to create in hardware.

Note: You must reboot the switch after giving this command for the changes to take effect.

Command Syntax

```
hardware-profile service-queue (profile1| profile2)
```

Parameter

`profile1`	Supports new 4 queue-bundle per service (default)
`profile2`	Supports new 8 queue-bundle per service

Default

By default, `profile1` is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile service-queue profile2
```

hardware-profile statistics

Use this command to enable or disable filter statistics in hardware.

Note: You must reboot the switch after giving this command for the changes to take effect.

Note: If both ACL and QOS statistics are required on the same interface, then both ingress-acl and ingress-qos profiles must be enabled and this will limit other profiles from being enabled. More details on restrictions explained below.

Note: When any two or all of MAC ACL or IP ACL or QoS service-policy are configured on the same interface, their entries will use statistics entries from ingress-acl statistics profile, and as a result the statistics is updated on only one entry based on the hardware-profile filter created later.

Command Syntax

```
hardware-profile statistics (ac-lif|cfm-ccm|cfm-lm|ingress-acl|ingress-qos|egress-
  acl|mpls-ac|mpls-lsp|mpls-pwe|tunnel-lif|voq-full-color|voq-fwd-drop)
  (enable|disable)
```

Parameter

`ac-lif`	VXLAN access ports statistics
`cfm-ccm`	Cfm ccm counter statistics
`cfm-lm`	Cfm Loss Measurements statistics
`tunnel-lif`	VXLAN tunnels statistics
`ingress-acl`	Ingress ACL, QoS, and PBR statistics
`ingress-qos`	Ingress QoS statistics (explicit)
`egress-acl`	Egress ACL statistics
`mpls-ac`	Attachment circuit statistics
`mpls-lsp`	LSP statistics
`mpls-pwe`	Pseudowire logical interfaces statistics
`voq-full-color`	Statistics for all VOQ counters
`voq-fwd-drop`	Statistics for forward drop VOQ counters
`enable`	Enable statistics
`disable`	Disable statistics

Default

By default, only `ingress-acl statistics` profile is enabled. Other statistics profiles are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```

```
(config)#hardware-profile statistics mpls-lsp enable
```

Table 2-48 provides details of scalable numbers of each statistics profiles and the applications that use the statistics profiles. For example, the `ingress-acl` profile is used by ACL, QoS, and PBR applications and all of them share the statistics entries from this profile. So, consuming 8k statistics entries for ACL application means that QOS and PBR applications do not get any statistics.

There are limitations on the number of statistics profiles that can be enabled at a time. This limitation is based on the stages that each profile uses. Table 2-48 shows the four stages: ingress, ingress queuing, egress1, and egress2; and only two statistics profiles per stage can be configured.

For example, if both the `ingress-acl` and `mpls-acl` profiles are configured, then no more profiles that use the "ingress stage" can be enabled because only two profiles are allowed per stage. To use another "ingress-based" profile, you must first disable at least one of the profiles that are currently using the ingress stage.

Table 2-48: Statistics profile capacity (maximum numbers in best case scenario)

Statistics profile	Stage	QMX	QAX	Application
ingress-acl	Ingress	~8k	~6k	Ingress ACL, QoS, PBR
egress-acl	Egress1	~8k	~2k	Egress ACL
ingress-qos	Ingress	~8k	~6k	QoS
voq-full-color	Ingress queuing	~13k	~6k	QoS (queue statictics)
voq-fwd-drop	Ingress queuing	~32k	~16k	QoS (queue statictics)
tunnel-lif	Ingress	~16k	N/A	VxLAN (tunnels)
	Egress2			
mpls-acl	Ingress	~32k	~8k	MPLS (attachment circuits)
	Egress2			
mpls-lsp	Ingress	~16k	~8k	MPLS (LSP/tunnel)
	Egress2			
mpls-pwe	Ingress	~16k	~8k	MPLS (pseudowire)
	Egress2			
cfm-ccm	Ingress	~3k	~800	CFM (ccm)
cfm-lm	Ingress	~6k	~1.5k	CFM (loss measurement)
	Egress2			
ac-lif	Ingress	~32k	N/A	VxLAN (access-port)
	Egress2			

ip urpf enable

Use this command to enable uRPF mode on the system.

Use the no form of the command to disable uRPF mode on this system.

Note: The configuration is applied only after a reboot.

Command Syntax

```
ip urpf enable
no ip urpf enable
```

Parameter

None

Default

By default, uRPF mode on the system is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip urpf enable
% System Reboot is required for new URPF configurations to take effect

(config)#no ip urpf enable
% System Reboot is required for new URPF configurations to take effect
```

ip urpf allow-default

Use this command to enable default route check for uRPF mode.

Use no form of this command to disable default route check for uRPF mode.

Command Syntax

```
ip urpf allow-default
no ip urpf allow-default
```

Parameter

None

Default

By default, uRPF mode is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip urpf allow-default

(config)#no ip urpf allow-default
```

ip mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes which allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the no form of this command to clear a multicast static route.

Command Syntax

```
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE)
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE) <1-
  255>
no ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|)
```

Parameters

NAME	Virtual Routing and Forwarding name
A.B.C.D/M	Multicast source IP address and mask of the source
static	Static routes.
rip	Routing Information Protocol.
ospf	Open Shortest Patch First protocol.
bgp	Border Gateway Protocol.
isis	Intermediate System to Intermediate System protocol.
A.B.C.D	IP address to use as the RPF address. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up to one level.
INTERFACE	Incoming interface name or pseudo interface null. Only specify for non-broadcast interfaces.
<1-255>	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip mroute 10.10.10.50/24 10.10.10.20 1
```

```
#configure terminal
(config)#ip mroute vrf VRF_A 10.10.10.50/1 10.10.10.20 1
```

ip redirects

Use this global command to trap ICMP redirect packets to the CPU and on interface to enable ICMP redirects in kernel.

Use the no form of this command to disable the ICMP redirect message on an interface.

Note: This command is applicable for both ipv4 and ipv6 interfaces.

Syntax

```
ip redirects
no ip redirects
```

Parameters

None

Default

None

Command Mode

Configure and Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#ip redirects


(config)#no ip redirects


#configure terminal
(config)#interface xe1/1
(config-if)#ip redirects


#configure terminal
(config)#interface xe1/1
(config-if)#no ip redirects
```

ipv6 mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the no form of this command to clear a multicast static route.

Command Syntax

```
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE
  <1-255>
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)
  <1-255>
no ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|)
```

Parameters

NAME	Virtual Routing and Forwarding name
X:X::X:X/M	Specify multicast source IP address and mask
static	Static routes.
rip	Routing Information Protocol.
bgp	Border Gateway Protocol.
ospf	Open Shortest Path First.
isis	Intermediate System to Intermediate System.
X:X::X:X	RPF address for the multicast route. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up one level.
INTERFACE	Incoming interface name. Can only be specified for non-broadcast interfaces.
<1-255>	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#ipv6 mroute 10:10::10:10/64 10:10::10:12 1
```

load-balance enable

Use this command to enable load-balancing configurations in hardware.

Use the no option to reset the load balancing to default settings.

Note: When the command "load-balance enable" is issued, the default load-balance settings are unset. User then has to configure the new load-balancing parameters.

Command Syntax

This form unsets load balancing globally:

```
load-balance enable
```

This form resets load balancing globally to default settings:

```
no load-balance enable
```

By default, load balancing is enabled for ECMP and LAG.

This form sets hashing based on IPv4 fields:

```
load-balance (ipv4 {src-ipv4 | dest-ipv4 | srcl4-port | destl4-port | protocol-id})
no load-balance (ipv4 {src-ipv4 | dest-ipv4 | srcl4-port | destl4-port | protocol-
  id})
```

This form sets hashing based on IPv6 fields:

```
load-balance (ipv6 {src-ipv6 | dest-ipv6 | srcl4-port | destl4-port | protocol-id})
no load-balance (ipv6 {src-ipv6 | dest-ipv6 | srcl4-port | destl4-port | protocol-
  id})
```

This form sets hashing based on L2 fields:

```
load-balance (l2 {dest-mac|src-mac|ether-type|vlan})
no load-balance (l2 {dest-mac|src-mac|ether-type|vlan})
```

This form sets hashing on an MPLS fields:

```
load-balance (mpls {labels})
no load-balance (mpls {labels})
```

Note: The configured load balancing parameters are global and will be applicable to all LAG & ECMP created in the hardware.

Parameters

`ipv4`	Load balance IPv4 packets
`src-ipv4`	Source IPv4 based load balancing
`dest-ipv4`	Destination IPv4 based load balancing

`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`protocol-id`	Protocol ID based load balancing
`ipv6`	Load balance IPv6 packets
`src-ipv6`	Source IPV6 based load balancing
`dest-ipv6`	Destination IPv6 based load balancing
`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`l2`	Load balance L2 packets
`dest-mac`	Destination MAC address based load balancing
`src-mac`	Source MAC address based load balancing
`ether-type`	Ether-type based load balancing
`Vlan`	VLAN-based load balancing
`mpls`	Load balance MPLS packets
`labels`	label stack based load balancing.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version SP 1.0.

Examples

```
(config)#load-balance enable
(config)#load-balance ipv4 src-ipv4
```

router-id

Use this command to add a router identifier for this system.

Use the no form of this command to disable this function.

Note: If router-id is not configured, highest ip address configured on the interface is chosen as router-id. if chosen ip address is unconfigured, make sure to execute clear router-id before configuring a new router-id.

Command Syntax

```
router-id A.B.C.D
no router-id (A.B.C.D)
```

Parameters

A.B.C.D	Router identifier in IP address format for this system.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router-id 123.12.3.123
(config)#
```

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax

```
show errdisable details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show errdisable details
```

show forwarding profile limit

Use this command to show all the forwarding profile table sizes.

Note: 1k is 1024 entries.

Command Syntax

```
show forwarding profile limit
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version SP 1.0.

Examples

```
OcNOS#show forwarding profile limit

-------------------------------------------------------------------------------
          L3 (Ipv4/Ipv6) KAPS Forwarding Profile
-------------------------------------------------------------------------------
Active (*)   Configured (*)  Profile-type     IPv4-db-size     IPv6-db-size
                             profile-one      NA               NA
   *           *             profile-two      -                200k

-------------------------------------------------------------------------------
          L3 (Ipv4/Ipv6) ELK TCAM Forwarding Profile
-------------------------------------------------------------------------------
Active (*)   Configured (*)  Profile-type     IPv4-db-size     IPv6-db-size
   *           *             profile-one      ~1024k           -
                             profile-two      -                ~1024k
                             profile-three    ~2048k           -

NOTE: for external-tcam profile-three, URPF should be disabled &
       number of vrf's limited to 255
-------------------------------------------------------------------------------
          L2 forwarding table
-------------------------------------------------------------------------------
            Max Entries: 768k

 NOTE: 1k is 1024 entries

OcNOS#
```

show hardware-profile filters

Use this command to show details of TCAM filter groups which are enabled. By default, all filter groups are disabled.

Command Syntax

```
show hardware-profile filters
```

Parameter

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#show hardware-profile filters

Note: Shared count is the calculated number from available resources.
      Dedicated count provides allocated resource to the group.
      If group shares the dedicated resource with other groups, then dedicated
      count of group will reduce with every resource usage by other groups.

+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10495     0     1         10486   2048        8448
```

Table 2-49 explains the output fields.

Table 2-49: show hardware-profile filters

Field	Description
Ingress	Ingress filtering is a method used to prevent suspicious traffic from entering a network.
TCAMS	Number of ternary content addressable memory (TCAM) entries a particular firewall filter.
Free Entries	Number of TCAM filter entries available for use by the filter group.
Used Entries	Number of TCAM filter entries used by the filter group.
Total Entries	Number of TCAM total filter entries to the filter group.

Table 2-49: show hardware-profile filters (Continued)

Field	Description
Dedicated Entries	Number of TCAM filter entries dedicated to the filter group.
Shared Entries	Number of TCAM filter entries shared to the filter groups.

Operational details of TCAM profiles

TCAM group statistics comprises of three parts:

- **Total Entries** – Total configurable entries on the TCAM group. Total has two parts. One is dedicated and other is shared. Dedicated count is the guaranteed entry count for the group. Shared count a logical count calculated for the group from shared pool available at the time of show command execution
- **Used Entries** – Count of entries that have been configured on the TCAM group. Used entries are shown are shown in percentage format as well as an indication of how much TCAM space is used up. However, percentage calculation includes shared pool and subject to change drastically when shared pool is taken up by different group.
- **Free Entries** – Count of possible remaining entries on the TCAM group. Free entries count is not the guaranteed count as the count includes the shared pool count into account.

When a TCAM group is enabled in the device, no hardware resource (bank) is associated with the group. Thus, dedicated count will be initially zero. Total count will be same as shared count which is calculated based on the group width. Group width is determined by width consumed by the qualifiers or width consumed by the actions.

Example of show output when qos-ext group is enabled on QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10496     0     0         10496   0           10496
```

When an entry is created on the group for the first time, either a single bank or a bank pair is allocated to the group. A group consuming single bank or a bank pair is decided by group width. Groups like qos, ingress-l2, ingress-ipv4, and forwarding-ipv4 consume single bank and groups like qos-ext, qos-policer, ingress-l2-ext, ingress-ipv4-ext, ingress-ipv4-qos, ingress-ipv6, ingress-ipv6-qos, egress-l2, and egress-ipv4 consume a bank pair.

An example of output when a single entry is created in hardware for qos-ext group on QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10495     0     1         10496   2048        8448
```

In the above example, dedicated entry count has increased to 2048 as a bank pair is allocated for the group. Unallocated banks capacity is calculated for qos-ext group and counted under shared entries as 8448.

An example of output when 2048 entries are created in hardware for qos-ext group and ingress-l2 and ingress-ipv4-ext groups is enabled with no entries created on those groups for QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      8448     20     2048      10496   2048        8448
 INGRESS L2           16896     0     0         16896   0           16896
 INGRESS IPV4-EXT     8448      0     0         8448    0           8448
```

In the above example, note that the number of entries between ingress-l2 and ingress-ipv4-ext groups vary as ingress-l2 group is a 160-bit wide group consuming only one bank at a time. On the other hand, ingress-ipv4-ext group is 320 bit wide group consuming a group pair at a time. With a bank pair already being consumed by qos-ext group, ingress-ipv4-ext group gets possible total entries of 8448 in comparison to 10496 by qos-ext group.

When all the created entry count goes beyond the entries of dedicated bank pair (or a bank), group will be allocated with another bank pair (or a bank) and subsequently shared pool count will reduce across all other groups.

An example of output when 2049 entries are created in hardware for qos-ext group with ingress-l2 and ingress-ipv4-ext groups enabled with no entries created on those groups for QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      8447      20    2049      10496   4096        6400
 INGRESS L2           12800     0     0         12800   0           12800
 INGRESS IPV4-EXT     6400      0     0         6400    0           6400
```

When a bank is consumed by ingress-l2 group, effect on qos-ext group will still be the count of a bank pair with one bank not usable for qos-ext group even if it is available. The bank can be used by groups which consume single bank.

An example of output when an entry is created in hardware for ingress-l2 group with qos-ext and ingress-ipv4-ext groups in the state as mentioned in above example is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      6399      24    2049      8448    4096        4352
 INGRESS L2           12799     0     1         12800   2048        10752
 INGRESS IPV4-EXT     4352      0     0         4352    0           4352
```

In the above example scenario, it can be noted that the used entry percentage for qos-ext group jumped from 20 to 24 as a result of drastic reduction in total entry count due to bank movement from shared pool to dedicated bank.

Hardware doesn’t optimize the utilization of banks when entries are removed from one of the banks resulting in entries used shown up less than capacity of one bank but still multiple banks would be dedicated to a group.

An extended example of above scenario with 10 entries removed from qos-ext group is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+---------------------------+
|                    | Free    |     Used      |       Total Entries       |
| TCAMS              | Entries |---------------|---------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      6409      24    2039      8448    4096        4352
 INGRESS L2           12799     0     1         12800   2048        10752
 INGRESS IPV4-EXT     4352      0     0         4352    0           4352
```

It can be noted that the used entry count has come down to 2039 which is less than the capacity of bank pair i.e. 2048. However, since entries are used up across two set of bank pairs, both bank pairs will still be dedicated. If there is a need to recover bank pair from dedicated pool, all the entries should be deleted and re-created in hardware.

TCAM groups are further divided into sub-categories which can share the dedicated banks between the groups. TCAM groups such as ingress-l2, ingress-l2-ext, ingress-ipv4, ingress-ipv4-ext, ingress-ipv4-qos, qos, qos-ext, qos-policer are considered under default sub-category and don't serve IPv6 traffic. TCAM groups such as ingress-ipv6, ingress-ipv6-qos, and qos-ipv6 are meant for IPv6 traffic and are considered under IPv6 sub-category.

Only four 320-bit wide groups that belong to same sub-category can be created. For default sub-category, number is limited to three as system group will be created by default.

When three default sub-category groups are created along with one group from IPv6 sub-category, one of the default sub-category group will share the bank pair with IPv6 group. This will result in dedicated count to be shown lesser by the number that the other shared group is consuming. With every single resource consumed by one group will reduce the same number from other shared group.

An example of above scenario is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+---------------------------+
|                    | Free    |     Used      |       Total Entries       |
| TCAMS              | Entries |---------------|---------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 QOS-EXT              6399      0     1         6400    2048        4352
 INGRESS IPV4-ACL-EXT 6398      0     2         6400    2048        4352
 INGRESS IPV4-QOS     6382      0     1         6383    2031        4352
 INGRESS IPV6-ACL     6382      0     17        6399    2047        4352
```

Note that ingress-ipv4-qos group has shared the resource with ingress-ipv6 group. TCAM group ingress-ipv4-qos has consumed 1 entry and ingress-ipv6 group has consumed 17 entries. Hence, dedicated count for ingress-ipv4-qos group is shown as 2031 (2048 - 17) and dedicated count for ingress-ipv6 group is shown as 2047 (2048 - 1).

Capacity of TCAM profiles

Entries created on other TCAM groups affect the capacity of a particular TCAM group. This dependency is explained in the section Operational details of TCAM profiles.

In this section maximum configurable entries per group when no entries created on other groups are listed below.

Table 2-50: Maximum configurable entries

TCAM Groups	QMX	QAX
ingress-l2	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)
ingress-l2-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 +256 x 1)
ingress-ipv4	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)
ingress-ipv4-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
ingress-ipv4-qos	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
ingress-ipv6	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
ingress-ipv6-qos	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
qos-ipv6	12288 (2048 x 6)	5120 (1024 x 5)
qos	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)
qos-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
qos-policer	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
forwarding-ipv4	41984 (4096 x 10 + 512 x 2)	19456 (2048 x 9 + 512 x 2)
egress-l2	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
egress-ipv4	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)
cfm-domain-name-str	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)

Combination of TCAM profiles

Device supports configuration of only one egress group in the system. Hence out of the egress groups cfm-domain-name-str, egress-l2 and egress-ipv4, only one egress group can be enabled.

In other words, solution with CFM features enabled, cannot have egress security filters.

Configuration of ingress groups are subject to the sub-category to which a group belongs. Sub-category of each group is shown below:

Table 2-51: Sub-category of groups

Category	Groups in the category
default (ingress)	ingress-l2 ingress-l2-ext ingress-ipv4 ingress-ipv4-ext ingress-ipv4-qos qos qos-ext qos-policer forwarding-ipv4
ipv6 (ingress)	ingress-ipv6, ingress-ipv6-qos, qos-ipv6
default (egress)	egress-l2, egress-ipv4
cfm (egress)	cfm-domain-name-str

Note: Per sub-category, not more than three groups can be created if the group key size is 320 bits wide.

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax

```
show interface errdisable status
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface errdisable status
ge1 lag-mismatch-errdisable
ge2 stp-bpdu-guard-errdisable
```

show queue remapping

Use this command to display the traffic class-to-hardware-queue mapping in hardware.

Command Syntax

```
show queue remapping
```

Parameters

N/A

Default

N/A

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

Examples

When service-queue `profile1` is set:

```
#show queue remapping

Port queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |          0            |
|      1     |          1            |
|      2     |          2            |
|      3     |          3            |
|      4     |          4            |
|      5     |          5            |
|      6     |          6            |
|      7     |          7            |
+------------+-----------------------+

Service queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |          0            |
|      1     |          1            |
|      2     |          1            |
|      3     |          1            |
```

```
|      4     |          2            |
|      5     |          2            |
|      6     |          3            |
|      7     |          3            |
+------------+-----------------------+
```

When service-queue `profile2` is set:

```
#show queue remapping

Port queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |          0            |
|      1     |          1            |
|      2     |          2            |
|      3     |          3            |
|      4     |          4            |
|      5     |          5            |
|      6     |          6            |
|      7     |          7            |
+------------+-----------------------+

Service queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |          0            |
|      1     |          1            |
|      2     |          2            |
|      3     |          3            |
|      4     |          4            |
|      5     |          5            |
|      6     |          6            |
|      7     |          7            |
+------------+-----------------------+
```

show router-id

Use this command to display the Router ID of the current system.

Command Syntax

```
show router-id
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show router-id
Router ID: 10.55.0.2 (automatic)
```

show running-config router-id

Use this command to show the running system global router ID configuration.

Command Syntax

```
show running-config router-id
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config router-id
!
router-id 3.3.3.3
!
```

show timezone

Use this command to display the list of timezone names.

Command Syntax

```
show timezone
  (all|africa|america|antarctica|arctic|asia|atlantic|australia|brazil|canada|chil
  e|europe|indian|mexico|pacific|us)
```

Parameters

`africa`	Africa timezone list
`all`	All timezone list
`l2-profile-three`	L2 profile Three (default); the size of the l2 table (Mac address table) and l3 table (Host table) is almost equal
`l3-profile`	L3 profile
`america`	America timezone list
`antarctica`	Antarctica timezone list
`asia`	Asia timezone list
`atlantic`	Atlantic timezone list
`australia`	Australia timezone list
`brazil`	Brazil timezone list
`canada`	Canada timezone list
`chile`	Chile timezone list
`europe`	Europe timezone list
`indian`	Indian timezone list
`mexico`	Mexico timezone list
`pacific`	Pacific timezone list
`us`	US timezone list

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show timezone asia
Asia:
Kuwait
```

```
Samarkand
Novosibirsk
Hebron
Singapore
Dushanbe
Rangoon
Riyadh
Thimphu
Shanghai
Phnom_Penh
Taipei
Qyzylorda
Ho_Chi_Minh
Urumqi
Chita
Khandyga
Nicosia
Jerusalem
Ashkhabad
Gaza
Tel_Aviv
Baghdad
Anadyr
Tehran
Ashgabat
Saigon
Damascus
Sakhalin
Yekaterinburg
Baku
Bangkok
Kashgar
Macao
Seoul
Jakarta
Aden
Katmandu
Amman
Ujung_Pandang
Kuching
Hong_Kong
Ulan_Bator
Dhaka
Macau
Omsk
Vientiane
Pyongyang
Ust-Nera
Manila
Srednekolymsk
Tbilisi
Kamchatka
Magadan
Istanbul
Chongqing
Jayapura
Yerevan
```

```
Makassar
Colombo
Karachi
Hovd
Novokuznetsk
Krasnoyarsk
Irkutsk
Kabul
Kolkata
Dacca
Brunei
Calcutta
Kathmandu
Bishkek
Qatar
Tashkent
Aqtau
Oral
Kuala_Lumpur
Pontianak
Harbin
Aqtobe
Bahrain
Muscat
Vladivostok
Dubai
Tokyo
Chungking
Almaty
Choibalsan
Thimbu
Beirut
Dili
Yakutsk
Ulaanbaatar
```

snmp restart

Use this command to restart SNMP for a given process.

Command Syntax

```
snmp restart (auth | bfd | bgp | cfm | efm | isis | ldp | lldp | mrib | mstp | nsm
  | ospf | ospf6 | pim | rib| rip | rmon | rsvp |vrrp)
```

Parameters

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart nsm
```

watch static-mac-movement

Use this command to watch any MAC movement is detected over static MAC entry for a time period. Notification will be displaying if static MAC movement happens till timer expires.

Command Syntax

```
watch static-mac-movement (<1-300>|)
```

Parameters

<1-300>	Timer value in second.

Default

By default, timer is 10 seconds

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#watch static-mac-movement
```

CHAPTER 3 Common Route-Map Mode Commands

This chapter is a reference for route-map commands. These commands are common to multiple protocols

This chapter includes the following commands:

- set origin
- set originator-id
- set tag
- set vpnv4 next-hop
- set weight
- show route-map
- show running-config route-map

continue

The continue clause provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses (i.e), the continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicate the order in which clauses are to be evaluated.

Use the no form of the command (specifying a particular sequence number if desired), to remove individual or all continue clauses from a route-map.

Continue clause with match Clauses

When a match clause exists in a route map with continue clause, then the continue clause is executed only when a successful match occurs. If a match clause does not exist in the route-map and if a continue clause does exist, the continue clause will be evaluated and then go to the specified route-map entry. When a successful match occurs and we have a continue clause, the route-map executes the set clauses and then goes to the specified route-map entry. If continue clause does not exist in the next route map, then the route-map will behave normally. If a continue clause exists in the next route-map but a match is not successful, the route-map will not continue and will *fall through* to the next sequence number if one exists.

Continue clause with set Clauses

Set clauses are executed after the route-map evaluation is done. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are only executed after a successful match occurs. The continue statement proceeds to the specified route-map entry only after configured set actions are performed. If a set action is configured in the first route-map and then the same set action occurs again, but with a different value in a subsequent route-map entry, then the last set action will override the previous set actions, which were configured with the same set command.

Command Syntax

```
continue <2-65535>|)
no continue <2-65535>|)
```

Parameter

<2-65535>	Continue sequence number.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#route-map Rmap1
(config-route-map)#continue ?
  <2-65535>  Route-map entry sequence number
  <cr>
(config-route-map)#continue 10
```

```
(config-route-map)#continue 30
```

match as-path

Use this command to match an autonomous system path access list. This command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are `not` met then the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove a path list entry.

Command Syntax

```
match as-path WORD
no match as-path (WORD|)
```

Parameter

`WORD`	Autonomous system path access list name.

Default

Enabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match as-path myaccesslist
```

match community

Use this command to specify the community to be matched.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by the `match community` command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax

```
match community (<1-99>|<100-199>|WORD) (exact-match|)
no match community (<1-99>|<100-199>|WORD|) (exact-match|)
```

Parameters

`<1-99>`	Community-list number (standard).
`<100-199>`	Community-list number (expanded).
`WORD`	Community-list name.
`exact-match`	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match community mylist
```

match extcommunity

Use this command to match BGP external community list

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by this command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the no parameter with this command to remove the community list entry.

Command Syntax

```
match extcommunity (<1-99>|<100-199>|WORD) (exact-match|)
no match extcommunity (<1-99>|<100-199>|WORD|) (exact-match|)
```

Parameters

<1-99>	Community-list number (standard).
<100-199>	Community-list number (expanded).
WORD	Name of the community-list.
exact-match	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match extcommunity mylist
```

match interface

Use this command to define the interface match criterion. This command specifies the next-hop interface name of a route to be matched.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax

```
match interface IFNAME
no match interface (IFNAME|)
```

Parameter

IFNAME	Interface name.

Default

By default, match interface is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match interface eth0
```

match ip address

Use this command to specify the match address of route. If there is a match for the specified IP address, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Command Syntax

```
match ip address (<1-199>|<1300-2699>|WORD)
no match ip address (<1-199>|<1300-2699>|WORD|)
```

Parameters

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match ip address List1
```

match ip address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the no parameter with this command too disable this function

Command Syntax

```
match ip address prefix-list WORD
no match ip address prefix-list (WORD|)
```

Parameter

WORD	IP prefix list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip address prefix-list mylist
```

match ip next-hop

Use this command to specify a next-hop address to be matched in a route-map. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the no parameter with this command to disable this function.

Command Syntax

```
match ip next-hop (<1-199>|<1300-2699>|WORD)
no match ip next-hop (<1-199>|<1300-2699>|WORD|)
```

Parameters

WORD	Specify the IP access-list name.
<1-199>	Specify the IP access-list number (standard range).
<1300-2699>	Specify the IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip next-hop mylist
```

match ip next-hop prefix-list

Use this command to specify the next-hop IP address match criterion using the prefix-list. This command matches the next-hop IP address of a route.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax

```
match ip next-hop prefix-list WORD
no match ip next-hop prefix-list (WORD|)
```

Parameter

WORD	Prefix-list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip next-hop prefix-list list1
```

match ip peer

Use this command to specify the match peer IPv4 address of a route.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax

```
match ip peer (<1-199>|<1300-2699>|WORD)
no match ip peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

WORD	IP access-list name.
<1-199>	IP access-list number (standard range).
<1300-2699>	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip peer 123

(config-route-map)#no match ip peer 123
```

match ipv6 address

Use this command to specify the match address of route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Command Syntax

```
match ipv6 address WORD
no match ipv6 address (WORD|)
```

Parameter

`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM deny 1
(config-route-map)#match ipv6 address myRM
```

match ipv6 address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Use the no parameter with this command to disable this function

Command Syntax

```
match ipv6 address prefix-list WORD
no match ipv6 address prefix-list (WORD|)
```

Parameter

WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 address prefix-list mylist
```

match ipv6 next-hop

Use this command to specify the next-hop address to be matched. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the no parameter with this command to disable this function

Command Syntax

```
match ipv6 next-hop (X:X::X:X|WORD)
no match ipv6 next-hop (X:X::X:X|WORD|)
```

Parameters

X:X::X:X	IPv6 address of the next-hop.
WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop 3ffe::1
```

match ipv6 next-hop prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the no parameter with this command to disable this function

Command Syntax

```
match ipv6 next-hop prefix-list WORD
no match ipv6 next-hop prefix-list WORD
```

Parameters

WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop prefix-list new
```

match ipv6 peer

Use this command to specify the match peer IPv6 address of a route.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax

```
match ipv6 peer (<1-199>|<1300-2699>|WORD)
no match ipv6 peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

WORD	IP access-list name.
<1-199>	IP access-list number (standard range).
<1300-2699>	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ipv6 peer 123

(config-route-map)#no match ipv6 peer 123
```

match metric

Use this command to match a metric of a route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPF, and IS-IS only.

Use the no parameter with this command to disable this function

Command Syntax

```
match metric <0-4294967295>
no match metric (<0-4294967295>|)
```

Parameters

`<0-4261412864>` Metric value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match metric 888999
```

match origin

Use this command to match origin code. The origin attribute defines the origin of the path information. The `egp` parameter is indicated as an `e` in the routing table, and it indicates that the origin of the information is learned via EGP (Exterior Gateway Protocol). The `igp` parameter is indicated as an `i` in the routing table, and it indicates the origin of the path information is interior to the originating AS. The `incomplete` parameter is indicated as a `?` in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

This command specifies the origin to be matched. If there is a match for the specified origin, and `permit` is specified when you created the route-map, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to disable this matching.

Command Syntax

```
match origin (egp|igp|incomplete)
no match origin (egp|igp|incomplete|)
```

Parameters

`egp`	Remote exterior gateway protocol.
`igp`	Local internal gateway protocol.
`incomplete`	Unknown heritage.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match origin egp
```

match route-type

Use this command to match an external route type. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes and external type-2 matches only Type 2 external routes.

Use the no parameter with this command to turn off the matching.

Command Syntax

```
match route-type external (type-1|type-2)
no match route-type external (type-1|type-2|)
```

Parameters

type-1	Match OSPF External Type 1 metric.
type-2	Match OSPF External Type 2 metric.

Default

By default, match route type external is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match route-type external type-1
```

match tag

Use this command to match the specified tag value.

Use the no parameter with this command to turn off the declaration.

Command Syntax

```
match tag <0-4294967295>
no match tag (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Tag value.

Default

By default, match tag is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match tag 100
```

route-map

Use this command to enter route-map mode and to permit or deny match/set operations.

This command controls and modifies routing information to allow redistribution of routes. It has a list of `match` and `set` commands associated with it. The `match` commands specify the conditions under which redistribution is allowed, and the `set` commands specify the particular redistribution actions to be performed if the criteria enforced by match commands are met. Route maps are used for detailed control over route distribution between routing processes.

Route maps also allow policy routing, and might route packets to a different route than the obvious shortest path.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax

```
route-map WORD (deny|permit) <1-65535>
no route-map WORD ((deny|permit) <1-65535>|)
```

Parameters

`WORD`	Route-map name (maximum size 63 characters).
`deny`	Route map deny set operations. If this parameter is specified, and the match criteria are met, the route is not redistributed, and any other route maps with the same map tag are not examined.
`permit`	Route map permit set operations. If this parameter is specified, and the match criteria are met, the route is redistributed as specified by the set actions. If the `match` criteria are not met, the next route map with the same tag is tested.
`<1-65535>`	Sequence to insert into or delete from an existing route-map.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map route1 permit 1
(config-route-map)#
```

set aggregator

Use this command to set the AS number for the route map and router ID. An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the `set aggregator` command to assign an AS number for the aggregator.

To use the `set aggregator` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to disable this function

Command Syntax

```
set aggregator as <1-65535> A.B.C.D
no set aggregator as (<1-65535> A.B.C.D|)
```

Parameters

`<1-65535>`	AS number of aggregator.
`A.B.C.D`	IP address of aggregator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set aggregator as 43 10.10.0.3
```

set as-path

Use this command to modify an autonomous system path for a route. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use this command to prepend an AS path string to routes increasing the AS path length.

To use this command, you must first give the `match` and `set` commands configure the conditions for redistributing routes from one routing protocol to another:

- The `match` command specifies the match criteria under which redistribution is allowed for the current route-map.
- The `set` command specifies the set redistribution actions to be performed if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set as-path prepend .<1-65535>
set as-path prepend .<1-4294967295>
no set as-path prepend (.<1-65535>|)
no set as-path prepend (.<1-4294967295>|)
```

Parameters

`<1-65535>`	OcNOS prepends this number to the AS path.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set as-path prepend 8 24
```

set atomic-aggregate

Use this command to set an atomic aggregate attribute.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to disable this function

Command Syntax

```
set atomic-aggregate
no set atomic-aggregate
```

Parameters

No default value is specified

Default

None

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set atomic-aggregate
```

set comm-list

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the no parameter with this command to disable this feature.

Command Syntax

```
set comm-list (<1-99>|<100-199>|WORD) delete
no set comm-list (<1-99>|<100-199>|WORD) delete
```

Parameters

<1-99>	Standard community-list number.
<100-199>	Expanded community-list number.
WORD	Name of the community-list.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM permit 3
(config-route-map)#set comm-list 34 delete
```

set community

Use this command to set the communities attribute. and group destinations in a certain community, as well as apply routing decisions according to those communities.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to delete the entry.

Command Syntax

```
set community [<65536-4294901759>|AA:NN|internet|local-AS|no-advertise|no-
  export|none] (additive|)
no set community [AA:NN|internet|local-AS|no-advertise|no-export|none] (additive|)
```

Parameters

`<65536-4294901759>`	Community number
`AA:NN`	The community number in aa:nn format.
`internet`	Internet.
`local-AS`	Do not send outside the local AS (well-known community).
`no-advertise`	Do not advertise this route to eBGP peers
`no-export`	Do not advertise this route to any peer.
`none`	Remove the community attribute from the prefixes that pass the route-map.
`additive`	Add to the existing community.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show the use of the `set community` command with different parameters.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-export no-advertise

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-advertise
```

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community 10:01 23:34 12:14 no-export
```

set dampening

Use this command to enable route-flap dampening and set parameters. Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Use the no parameter with this command to delete the entry.

Command Syntax

```
set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
no set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
```

Parameters

<1-45>	Reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value.
<1-20000>	Reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
<1-20000>	Suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed.
<1-255>	Max-suppress-time. Maximum time that a dampened route is suppressed.
<1-45>	Unreachability half-life time for penalty, in minutes.

Default

Default reachability half-life time: 15 minutes

Default reuse limit value: 750

Default suppress limit value: 2000

Default max-suppress value is 4 times the half-life time (60 minutes)

Default unreachability half-life time value: 15 minutes

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map R1 permit 24
(config-route-map)#set dampening 20 333 534 30
```

set extcommunity

Use this command to set an extended community attribute.

To use this command you must first have a match clause. The `match` and `set` commands define the conditions for redistributing routes from one routing protocol to another:

- The `match` command defines the match criteria under which redistribution is allowed for the current route-map.
- The `set` command defines the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set extcommunity rt .AA:NN (additive|)
set extcommunity soo .AA:NN
set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
no set extcommunity rt (.AA:NN|) (additive|)
no set extcommunity soo (.AA:NN|)
no set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
```

Parameters

`rt`	Route target extended community.
`.AA:NN`	VPN extended community
`additive`	Add to the exsisting community.
`soo`	Site-of-origin extended community.
`cost`	Extended cost community.
`igp`	Compare following IGP cost comparison.
`pre-bestpath`	Compare following IGP cost comparison.
`<0-255>`	Community ID.
`<0-4294967295>`	Cost.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 06:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 0.0.0.6:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 06:01

#configure terminal
(config-route-map)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 0.0.0.6:01
```

set interface null0

Use this command to discard routes based on policy/rules configured for a route map.

Route maps can be applied to BGP neighbors. When this command is given for a route map and that route map is applied to a BGP neighbor, the discard route entries are added by BGP for the prefix permitted by the route map.

Use the no form of this command to not discard routes based on policy/rules configured for a route map.

Command Syntax

```
set interface null0
no set interface null0
```

Parameters

None

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

To discard 1.1.1.1/24 from BGP neighbor 30.1.1.1:

```
#configure terminal
(config)#ip prefix-list myPrefixList seq 5 permit 1.1.1.1/24 eq 24
(config)#route-map myRM permit 1
(config-route-map)#match ip address prefix-list myPrefixList
(config-route-map)#set interface null0
(config-route-map)#exit
(config)#router bgp 200
(config-router)#neighbor 30.1.1.1 remote-as 200
(config-router)#neighbor 30.1.1.1 route-map myRM in
```

set ip next-hop

Use this command to set the specified next-hop value.

Use the no parameter with this command to turn off the setting.

Note: This command is valid for BGP and OSPF only.

Command Syntax

```
set ip next-hop A.B.C.D
no set ip next-hop (A.B.C.D|)
```

Parameter

A.B.C.D	IP address of the next-hop.

Default

By default, set ip next hop A.B.C.D is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#set ip next-hop 10.10.0.67
```

set ipv6 next-hop

Use this command to set a next hop-address.

Use the no parameter with this command to delete an entry.

Note: This command is valid for BGP and OSPFv3 only.

Command Syntax

```
set ipv6 next-hop X:X::X:X
set ipv6 next-hop local X:X::X:X
no set ipv6 next-hop (X:X::X:X|)
no set ipv6 next-hop local (X:X::X:X|)
```

Parameters

X:X::X:X	Global IPv6 address of the nexthop.
local	Local IPv6 address of the nexthop.

Default

By default, set ipv6 next hop X:X::X:X is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set ipv6 next-hop local fe80::203:47ff:fe97:66dc
```

set level

Use this command to set the IS-IS level to export a route.

Use the no parameter with this command to disable this function.

Command Syntax

```
set level (level-1|level-2|level-1-2)
no set level (level-1|level-2|level-1-2|)
```

Parameters

`level-1`	Export into a level-1 area.
`level-2`	Export into a level-2 sub-domain.
`level-1-2`	Export into level-1 and level-2.

Default

By default, set level is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set level level-1
```

set local-preference

Use this command to set the BGP local preference path attribute.

Use the no parameter with this command to disable this function.

Command Syntax

```
set local-preference <0-4294967295>
no set local-preference (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Tag value for destination routing protocol.

Default

By default, set local preference is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set local-preference 12
```

set metric

Use this command to set a metric value for a route and influence external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the `bgp always-compare-med` command.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set metric WORD
no set metric (WORD|)
```

Parameters

`WORD`	Metric value [+/-] <1-4294967295>

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric 600
```

set metric-type

Use this command to set the metric type for the destination routing protocol. Select a type to be either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Note: This command is for OSPF, OSPFv3, or IS-IS only.

Use the no parameter with this command to return to the default.

Command Syntax

```
set metric-type (internal|external)
set metric-type (type-1|type-2)
no set metric-type (internal|external|)
no set metric-type (type-1|type-2|)
```

Parameters

external	IS-IS external metric type.
internal	IS-IS internal metric type.
type-1	OSPF external type 1 metric.
type-2	OSPF external type 2 metric

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In this example the metric type of the destination protocol is set to OSPF external Type 1.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric-type 1
```

set origin

Use this command to set the BGP origin code. The origin attribute defines the origin of the path information.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to delete an entry.

Command Syntax

```
set origin (egp|igp|incomplete)
no set origin (egp|igp|incomplete|)
```

Parameters

`egp`	Learned through an Exterior Gateway Protocol.
`igp`	Interior to the originating AS. This happens when an Internal Gateway Protocol is redistributed into BGP.
`incomplete`	Unknown or learned through some other means. This happens when a static route is redistributed in BGP and the origin of the route is incomplete.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set origin egp
```

set originator-id

Use this command to set the originator ID attribute.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set originator-id A.B.C.D
no set originator-id (A.B.C.D|)
```

Parameter

`A.B.C.D`	IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set originator-id 1.1.1.1
```

set tag

Use this command to set a tag value. The parameter is the route tag that is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. In addition, when using route-map, OcNOS can tag the LSAs with the appropriate tag value. Sometimes the tag matches with using route-map, and sometimes, the value may be used by another application.

Use the no parameter with this command to unset a tag value.

Command Syntax

```
set tag <0-4294967295>
no set tag (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Tag value for destination routing protocol.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example the tag value of the destination routing protocol is set to 6:

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set tag 6
```

set vpnv4 next-hop

Use this command to set a VPNv4 next-hop address.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Note: This command is valid for BGP only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set vpnv4 next-hop A.B.C.D
no set vpnv4 next-hop (A.B.C.D|)
```

Parameter

`A.B.C.D`	IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set vpnv4 next-hop 6.6.6.6
```

set weight

Use this command to set weights for the routing table.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to delete an entry.

Command Syntax

```
set weight <0-4294967295>
no set weight (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Weight value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration, all routes that apply to access-list 10 will have the weight set at 400. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match as-path 10
(config-route-map)#set weight 400
```

show route-map

Use this command to display route-map information.

Command Syntax

```
show route-map (|WORD)
```

Parameters

WORD	Route-map name (maximum size 63 characters)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show route-map` command.

```
#show route-map
route-map myRM, permit, sequence 1
  Match clauses:
    metric 200
  Set clauses:
    metric 60
#
```

Table 3-52 explains the output fields.

Table 3-52: show route-map details

Field	Description
route-map	Name of a route map.
permit	Routes that match the match clauses are redistributed according to the conditions defined by the set clauses.
sequence	Position of this route map in sequence of route-maps with the same name.
Match clauses	Routes that match the conditions defined by the match clause are redistributed according to the conditions defined by the set clauses.
Set clauses	Routes that pass the match clause are redistributed according to the conditions defined by the set clauses.

show running-config route-map

Use this command to display the running system status and configuration details for route-maps.

Command Syntax

```
show running-config route-map
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config route-map
!
route-map abc deny 2
 match community 2
!
route-map abc permit 3
 match route-type external type-2
 set metric-type type-1
!
```

CHAPTER 4 Interface Commands

This chapter is a reference for each of the interface commands.

- ipv6 nd retransmission-time
- ipv6 nd suppress-ra
- ipv6 prefix-list
- ipv6 unnumbered
- link-flap errdisable
- load interval
- monitor speed
- monitor queue-drops
- monitor speed threshold
- mtu
- multicast
- port breakout enable
- port bundle enable
- protocol-control
- show hardware-discard-counters
- show interface
- show interface counters
- show interface counters drop-stats
- show interface counters error-stats
- show interface counters (indiscard-stats|outdiscard-stats)
- show interface counters protocol
- show interface counters queue-drop-stats
- show interface counters queue-stats
- show interface counters rate
- show interface counters speed
- show interface counters summary
- show interface protocol-control status
- show ip forwarding
- show ip interface
- show ip prefix-list
- show ip route
- show ip vrf
- show ipv6 forwarding
- show ipv6 interface brief
- show ipv6 route
- show ipv6 prefix-list
- show hosts
- show running-config interface
- show running-config interface ip

- show running-config interface ipv6
- show running-config ip
- show running-config ipv6
- shutdown
- speed
- switchport
- switchport allowed ethertype

admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in configure mode, then interfaces are added to the group in interface mode.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
admin-group NAME
no admin-group NAME
```

Parameters

`NAME`	Name of the admin group to add.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the `eth3` interface is added to the group `myGroup`:

```
#configure terminal
(config)#interface eth3
(config-if)#admin-group myGroup
```

bandwidth

Use this command to specify a discrete, maximum bandwidth value for the interface.

Use the no parameter resets the interface's bandwidth to the default value.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameter

BANDWIDTH	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

Default bandwidth will be default speed of the interface. For LAG, default bandwidth will be collective bandwidth of its member ports. For VLAN interface, default bandwidth is 1 gigabits/sec.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe4
(config-if)#bandwidth 100m
```

clear hardware-discard-counters

Use this command to clear device level discard counters.

Command Syntax

```
clear hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Examples

```
#clear hardware-discard-counters
```

clear interface counters

Use this command to clear the statistics on a specified interface or on all interfaces.

Note: This command is not supported on loopback interfaces or the out-of-band management (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) counters
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface xe0 counters
```

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax

```
clear interface cpu counters
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface cpu counters
```

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

Command Syntax

```
clear ip prefix-list
clear ip prefix-list WORD
clear ip prefix-list WORD A.B.C.D/M
```

Parameters

WORD	Name of the prefix-list.
A.B.C.D/M	IP prefix and length.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip prefix-list List1
```

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Command Syntax

```
clear ipv6 neighbors
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 neighbors
```

clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

Command Syntax

```
clear ipv6 prefix-list
clear ipv6 prefix-list WORD
clear ipv6 prefix-list WORD X:X::X:X/M
```

Parameters

WORD	Name of the prefix-list.
X:X::X:X/M	IP prefix and length.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 prefix-list List1
```

debounce-time

Use this command to set the debounce time for a interface.

The debounce timer avoids frequent updates (churn) to higher layer protocol during interface flapping. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce is not applicable for admin down operations.
- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to a minimum of 1.5 times the value of the debounce timer. Otherwise it could affect the protocol states if the debounce timer is still running.

Use the no form of this command to turn-off the debounce timer on a interface.

Command Syntax

```
debounce-time <250-5000>
no debounce-time
```

Parameters

<250-5000>	Timer value in milliseconds.

Default

By default, disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#debounce-time 4000
```

description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Interface description.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router#configure terminal
Router(config)#interface eth1
Router(config-if)#description Connected to Zenith's fas2/0
```

duplex

Use this command to set the duplex mode for each interface.

Use the no parameter to remove the duplex mode.

Command Syntax

```
duplex (half|full)
no duplex
```

Parameter

`half`	Half-duplex mode.
`full`	Full-duplex mode.

Default

By default, duplex mode is full duplex.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#duplex full

(config-if)#no duplex
```

fec

Use this command to configure forward error correction (FEC) on a physical port.

Use no parameter to un-configure FEC.

Command Syntax

```
fec (on|auto)
no fec
```

Parameter

on	Enable FEC.
auto	Enable FEC with autonegotiation.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#fec on

(config-if)#no fec
```

hardware-profile portmode

Use this command to set the global port mode.

Command Syntax

```
hardware-profile portmode (4X10g|40g)
```

Parameter

`4X10g`	Split all the 40G flex ports on the system
`40g`	Disable splitting on all flex ports and make all ports 40G

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#hardware-profile portmode 40g
```

hardware-profile portmode bundle

Use this command to set the global port mode to bundle.

Command Syntax

```
hardware-profile portmode bundle (40g|4X10g)
```

Parameter

`40g`	Bundle four 10G ports to a single 40G port
`4x10g`	Unbundle ports

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#hardware-profile portmode bundle 40g
(config)#exit
(config)#hardware-profile portmode bundle 4x10g
(config)#exit
```

if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the OcNOS database.

This command starts the arbiter to check interface information periodically. OcNOS dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when OcNOS is already running, this command polls and updates the kernel information periodically.

Use the no parameter with this command to revert to default.

Command syntax

```
if-arbiter (interval <1-65535>|)
no if-arbiter
```

Parameter

`interval`	Interval (in seconds) after which NSM sends a query to the kernel.

Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of OcNOS (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `noif-arbiter` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#if-arbiter interval 5
```

interface

Use this command to select an interface to configure, and to enter the `Interface` command mode.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
interface IFNAME
no interface IFNAME
```

Parameter

`IFNAME`	Name of the interface.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

```
#configure terminal
(config)#interface eth3
(config-if)#
```

ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the no parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address A.B.C.D/M label LINE
ip address A.B.C.D/M (secondary|)
ip address A.B.C.D/M secondary label LINE
no ip address A.B.C.D/M label LINE
no ip address A.B.C.D/M secondary label LINE
no ip address (A.B.C.D/M (secondary|)|)
```

Parameters

`LINE`	Label of this address.
`secondary`	Make the IP address secondary.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```

ip address dhcp

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the no parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

ip forwarding

Use this command to turn on IP forwarding.

Use the no parameter with this command to turn off IP forwarding.

Command Syntax

```
ip forwarding
ip forwarding vrf NAME
no ip forwarding
no ip forwarding vrf NAME
```

Parameters

NAME	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip forwarding
```

ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

Use the parameters `ge` and `le` specify the range of the prefix length to be matched. When setting these parameters, set `le` to be less than 32 and `ge` to be less than `le` value.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ip prefix-list WORD (deny|permit) (A.B.C.D/M|any)
ip prefix-list WORD (deny|permit) A.B.C.D/M eq <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
no ip prefix-list WORD
no ip prefix-list WORD (deny|permit) (A.B.C.D/M|any)
no ip prefix-list WORD (deny|permit) A.B.C.D/M eq <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-
  32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-
  32>
ip prefix-list sequence-number
no ip prefix-list sequence-number
```

```
ip prefix-list WORD description LINE
no ip prefix-list WORD description LINE
no ip prefix-list WORD description
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`A.B.C.D/M`	IP address mask and length of the prefix list mask.
`eg`	Exact prefix length match
`le`	Maximum prefix length match
`ge`	Minimum prefix length match
`<0-32>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`any`	Take all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for `A.B.C.D/M`.
`sequence-number`	To suppress sequence number generation, give the `no ip prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ip prefix-list` command. To enable sequence number generation, give the `ip prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
(config-router)#neighbor 10.6.5.3 prefix-list mylist out
(config-router)#exit
(config)#ip prefix-list mylist seq 5 deny 76.2.2.0/24
```

```
(config)#ip prefix-list mylist seq 10 permit 0.0.0.0/0
```

ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the no parameter to disable the proxy ARP feature on an interface.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameters

None

Default

By default, the ip proxy-arp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip proxy-arp
```

ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the no parameter to disable this function.

Command Syntax

```
ip remote-address A.B.C.D/M
no ip remote-address
```

Parameter

A.B.C.D/M	IP address and prefix length of the link remote address.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```

ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link. Moreover, this command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-to-point interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax

```
ip unnumbered IFNAME
no ip unnumbered
```

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example creates a tunnel on `eth1`.

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

ip vrf forwarding

This command associates an interface with a VRF.

Use the no parameter with this command to unbind an interface.

Note: When you give this command in interface configuration or subinterface configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving this command, the IP attributes must then be configured in the context of the VRF.

Note: The Out Of Band (OOB) management port is part of the “management” VRF. Also, this port cannot be moved out of “management” VRF.

Command Syntax

```
ip vrf forwarding WORD
no ip vrf forwarding WORD
```

Parameter

WORD	Name of the VRF.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#exit
(config)#interface eth1
(config-if)#ip vrf forwarding myVRF
```

ipv6 address

Use this command to set the IPv6 address of an interface.

Use the no form of this command to disable this function.

Command Syntax

```
ipv6 address X:X::X:X/M
ipv6 address X:X::X:X/M anycast
no ipv6 address X:X::X:X/M
```

Parameters

`X:X::X:X/M`	IP destination prefix and a mask length.
`anycast`	Make an anycast address which is assigned to a set of interfaces that belong to different devices. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 address 3ffe:506::1/64
```

ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the no parameter with this command to turn off IPv6 forwarding.

Command Syntax

```
ipv6 forwarding
ipv6 forwarding vrf NAME
no ipv6 forwarding
no ipv6 forwarding vrf NAME
```

Parameters

NAME	Virtual Routing or Forwarding name

Default

No default value is specified

Command Mode

Command mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 forwarding
```

ipv6 nd current-hoplimit

Use this command to set an ND (Neighbor Discovery) advertised hop limit for an interface.

Use the no option of this command to set the current hop limit to its default value.

Command Syntax

```
ipv6 nd current-hoplimit <0-255>
no ipv6 nd current-hoplimit
```

Parameter

<0-255>	Hop limit.

Default

By default, hop limit is 64

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd current-hoplimit 10
(config-if)#no ipv6 nd current-hoplimit
```

ipv6 nd link-mtu

Use this command to set an advertised maximum transmission unit (MTU).

Use the no option with the command to reset the MTU to the default statute.

Command Syntax

```
ipv6 nd link-mtu (<1280-65535>)
no ipv6 nd link-mtu
```

Parameters

<1280-65535>	Link MTU value.

Default

By default, link MTU value is 1500

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd link-mtu 1600
(config-if)#no ipv6 nd link-mtu
```

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag in the Router Advertisement to be used for the IPv6 address auto-configuration.

Use the no parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Parameters

None

Default

The managed address configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd managed-config-flag
(config-if)#no ipv6 nd managed-config-flag
```

ipv6 nd minimum-ra-interval

Use this command to set a minimum Router Advertisement (RA) interval for the interface.

Use the no option with the command to set the RA interval to its default value.

Command Syntax

```
ipv6 nd minimum-ra-interval <3-1350>
no ipv6 nd minimum-ra-interval (<3-1350>|)
```

Parameter

<3-1350>	Minimum RA interval (in seconds).

Default

By default, RA interval is 180 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd minimum-ra-interval 400
(config-if)#no ipv6 nd minimum-ra-interval
```

ipv6 nd other-config-flag

Use this command to set the other stateful configuration flag in Router Advertisement to be used for IPv6 address auto-configuration.

Use no parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Parameters

None

Default

Other stateful configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd other-config-flag
(config-if)#no ipv6 nd suppress-ra
```

ipv6 nd prefix

Use this command to set IPv6 prefix information that is advertised for address auto-configuration.

Use no parameter with this command to remove an IPv6 prefix.

Command Syntax

```
ipv6 nd prefix X:X::X:X/M <0-4294967295> <0-4294967295> (off-link|) (no-
  autoconfig|)
ipv6 nd prefix X:X::X:X/M
ipv6 nd prefix valid-lifetime <0-4294967295>
ipv6 nd prefix preferred-lifetime <0-4294967295>
ipv6 nd prefix offlink
ipv6 nd prefix no-autoconf
no ipv6 nd prefix X:X::X:X/M
no ipv6 nd prefix valid-lifetime (<0-4294967295>|)
no ipv6 nd prefix preferred-lifetime (<0-4294967295>|)
no ipv6 nd prefix offlink
no ipv6 nd prefix no-autoconf
```

Parameters

`X:X::X:X/M`	IPv6 prefix.
`<0-4294967295>`	Valid lifetime in seconds.
`<0-4294967295>`	Preferred lifetime in seconds.
`off-link`	Do not use prefix for onlink determination.
`no-autoconfig`	Do not use prefix for autoconfiguration.

Default

By default, valid life time is 2592000 seconds and preferred life time is 604800 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Defaults

The default valid lifetime is 2592000 seconds.

The default preferred lifetime is 604800 seconds.

Examples

```
(config)#interface eth3
(config-if)#ipv6 nd prefix 2001:ffff::/64
```

```
(config)#interface eth3
(config-if)#ipv6 nd prefix no-autoconf

(config)#interface eth3
(config-if)#ipv6 nd prefix preferred-lifetime 550000
```

ipv6 nd ra-interval

Use this command to specify the interval between IPv6 Router Advertisements (RA).

Use no parameter with this command to set the value to its default.

Command Syntax

```
ipv6 nd ra-interval <4-1800>
no ipv6 nd ra-interval
```

Parameter

<4-1800>	RA interval in milliseconds.

Default

By default, RA interval is 600 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-interval 60
(config-if)#ipv6 nd prefix 3ffe:ffff:ffff::/64

(config-if)#no ipv6 nd ra-interval
```

ipv6 nd ra-lifetime

Use this command to specify the Router Advertisement (RA) lifetime for this device to act as a default gateway for the network.

Use no parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd ra-lifetime <0-9000>
no ipv6 nd ra-lifetime
```

Parameter

<0-9000>	RA lifetime duration in seconds.

Default

The default RA lifetime is 1800 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-lifetime 9000
(config-if)#no ipv6 ra-lifetime 9000
```

ipv6 nd reachable-time

Use this command to specify the reachable time in the Router Advertisement to be used for detecting unreachability of the IPv6 neighbor.

Use the no parameter with this command to set the value to its default.

Command Syntax

```
ipv6 nd reachable-time <0-3600000>
no ipv6 nd reachable-time
```

Parameter

<0-3600000>	Reachable time in milliseconds.

Default

By default, reachable time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd reachable-time 1800000
(config-if)#no ipv6 nd reachable-time 1800000
```

ipv6 nd retransmission-time

Use this command to set an IPv6 advertised retransmission time for the current interface.

Use the no form of the command to set the retransmission time to its default value.

Command Syntax

```
ipv6 nd retransmission-time (0-4294967295)
no ipv6 nd retransmission-time
```

Parameter

`<0-4294967295>` Retransmission time in milliseconds

Default

By default, retransmission time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd retransmission-time 1200
(config-if)#no ipv6 nd retransmission-time
```

ipv6 nd suppress-ra

Use this command to suppress IPv6 Router Advertisement (RA) transmission for the current interface. Router Advertisement is used for IPv6 stateless auto-configuration.

Use the no parameter with this command to enable Router Advertisement transmission.

Command Syntax

```
ipv6 nd suppress-ra (mtu |)
no ipv6 nd suppress-ra (mtu |)
```

Parameters

mtu	Do not send maximum transmission unit (MTU) in Router Advertisement messages

Default

By default, ipv6 nd suppress-ra is suppressed

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd suppress-ra
```

ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `ge` and `le` specify the range of the prefix length to be matched.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any)
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-
  128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-
  128>
no ipv6 prefix-list WORD
no ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any)
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le
  <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge
  <0-128>
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number
ipv6 prefix-list WORD description LINE
no ipv6 prefix-list WORD description
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`X:X::X:X/M`	IP address mask and length of the prefix list mask.
`any`	Take all packets of any length. This is the same as specifying ::/0 for X:X::X:X/M.
`eg`	Exact prefix length match
`le`	Maximum prefix length match
`ge`	Minimum prefix length match
`<0-128>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`sequence-number`	To suppress sequence number generation, give the `no ipv6 prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ipv6 prefix-list` command. To enable sequence number generation, give the `ipv6 prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist seq 12345 deny 3ffe:345::/16 le 22 ge 14
```

ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a point-to-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the no parameter with this command to remove this feature on an interface.

Command Syntax

```
ipv6 unnumbered IFNAME
no ipv6 unnumbered
```

Parameter

IFNAME	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example creates a tunnel on eth1:

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

link-flap errdisable

Use this command to shut down the interface when it continually goes up and down.

The link-flap ErrDisable feature must be enabled globally with the errdisable cause command.

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: This feature is supported only on physical ports.

Use the `no` form of this command to disable this behavior.

Command Syntax

```
link-flap errdisable
no link-flap errdisable
```

Parameter

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#link-flap errdisable
```

load interval

Use this command to configure the interval for which average traffic rate need to be shown. Intervals can be configured in steps of 30 seconds.

Use the no parameter with this command to set the load interval to its default.

Command Syntax

```
load-interval <30-300>
no load-interval
```

Parameter

<30-300>	Load period in multiples of 30 seconds.

Default

By default, load interval is 300 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#load-interval 30
(config-if)#no load-interval
```

monitor speed

Use this command to enable speed monitoring on interface.

Use the no parameter with this command to disable monitoring.

Command Syntax

```
monitor speed
no monitor speed
```

Default

By default, speed monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor speed
(config-if)#no monitor speed
```

monitor queue-drops

Use this command to enable queue-drops monitoring on interface.

Use the no parameter with this command to disable monitoring.

Command Syntax

```
monitor queue-drops
no monitor queue-drops
```

Default

By default, queue-drops monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor queue-drops
(config-if)#no monitor queue-drops
```

monitor speed threshold

Use this command to modify default speed monitor threshold on interface.

Use the no parameter with this command to set the monitor speed threshold to its default.

Note: Warning threshold must be greater than recovery threshold and it is recommended to keep a difference of 10 percent to avoid frequent notifications caused by variations in average speed.

Command Syntax

```
monitor speed threshold warning <1-100> recovery <1-100>
no monitor speed threshold
```

Parameter

<1-100>	Warning level threshold value in percentage
<1-100>	Recovery level threshold value in percentage

Default

By default, warning threshold is 90 percentage and recovery is 80 percentage.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)# monitor speed threshold warning 80 recovery 70
(config-if)#no monitor speed threshold
```

mtu

Use this command to set the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) for an interface

Use the no parameter with this command to set the MTU to its default.

Command Syntax

```
mtu <64-65536>
no mtu
```

Parameter

<64-65536>	Specify the size of MTU in bytes: <64-16338> for L2 packet <576-9216> for L3 IPv4 packet <1280-9216> for L3 IPv6 packet <576-65536> for IPv4 packet <1280-65536> for IPv6 packet on loopback interface

Default

By default, MTU is 1500 bytes

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#mtu 120
```

multicast

Use this command to set the multicast flag for the interface.

Use the no form of this command to disable this function.

Command Syntax

```
multicast
no multicast
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#multicast
```

port breakout enable

Use this command to split a 40G interface to four 10G interfaces or 100G interface to four 10G or four 25G or two 50G interfaces without restarting the device.

You can only break out controlling ports. For example, in the group that contains the `xe1/1`, `xe1/2`, `xe1/3`, and `xe1/4` interfaces, the `xe1/1` interface is the controlling port (first port in the group) and `xe1/2`, `xe1/3`, and `xe1/4` are subsidiary ports (non control ports).

Ports that support the breakout feature display with a "/" in their name. By default, only control ports are active (/1) and remaining ports (/2, /3, and /4) are inactive.

Use the `show interface brief` command to verify if a port is controlling or subsidiary. You can also use the `show interface` command to check the flexport status. The status would be one of the below:

```
Flexport: Control Port (Active): Break Out disabled
Flexport: Control Port (Active): Break Out Enabled
Flexport: Non Control Port (InActive)
Flexport: Non Control Port (Active)
```

The output from commands such as `show running-config` reflect the split port configuration.

The bandwidth of a controlling port is reset to its maximum allowed speed after a split is enabled or disabled.

Any pre-configuration of the subsidiary port is applied directly once it becomes active.

Use the `no` form of this command to return the interface to single-port, 40G/100G operation.

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.

Command Syntax

40G port:

```
port breakout enable
no port breakout
```

100G port:

```
port breakout enable (4x10g|4x25g|2x50g)
no port breakout
```

Parameters

`<4x10g>`	Split 100G to 4X10g
`<4x25g>`	Split 100G to 4X25g
`<2x50g>`	Split 100G to 2X50g

Default

By default, only control ports are active (/1) and remaining ports (/2, /3, and /4) are inactive.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to split a 40G port:

```
#configure terminal
(config)#interface xe1/1
(config-if)#port breakout enable
(config-if)#end

#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
forwarding profile l2-profile-two
ip domain-lookup
bridge 1 protocol rstp vlan-bridge
data-center-bridging enable bridge 1
ethernet cfm enable
!

!
interface xe1/1
 port breakout enable
 switchport
 bridge-group 1
 switchport mode access
 channel-group 1 mode active
!
interface xe1/2
 speed 1g
!
interface xe1/3
 speed 1g
 switchport
 bridge-group 2
 switchport mode trunk
!
interface xe1/4
!
```

This example shows how to split a 100G port:

```
#configure terminal
(config)#interface ce1/1
(config-if)#port breakout enable ?
  2X50g  split to 2X50g
  4X10g  split to 4X10g
  4X25g  split to 4X25g
(config-if)#port breakout enable 4X25g
(config-if)#end
#show running-config
```

```
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
forwarding profile l2-profile-two
ip domain-lookup
bridge 1 protocol rstp vlan-bridge
data-center-bridging enable bridge 1

ethernet cfm enable
!
interface ce1/1
port breakout enable 4X25g
```

Similarly, a 100G port can be split into 4x10G ports or 2x50G ports.

port bundle enable

Use this command to bundle four 10G SFP+ interfaces into a single 40G interface without restarting the device. You can use this command only on bundle control ports.

For example, if the xe1 interface is bundle control port then this command can be used and following three ports xe2, xe3, and 4 would be subsidiary ports (non control ports) and would become inactive.

Use the show interface brief command to verify if a port is bundle controlling or subsidiary. You can also use the show interface command to check the flexport status. The status would be one of the below:

Flexport: Bundle Control Port (Active): Bundle disabled

Flexport: Bundle Control Port (Active): Bundle Enabled

Flexport: Non Control Port (InActive)

Flexport: Non Control Port (Active)

The output from commands such as show running-config reflect the bundle port configuration.

Use the no form of this command to revert to four 10G ports.

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.

Command Syntax

```
port bundle enable
no port bundle
```

Parameters

None

Default

By default, ports are not bundled and all the ports are active (xe1, xe2, xe3, and xe4).

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to split a 40G port:

```
#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
```

```
!
forwarding profile l2-profile-two
ip domain-lookup
bridge 1 protocol rstp vlan-bridge
data-center-bridging enable bridge 1
ethernet cfm enable
!
!
interface xe1
port bundle enable
!
interface xe2
!
interface xe3
!
interface xe4
!
```

protocol-control

Use this command to enable/disable lifting L3 control packets to CPU.

Command Syntax

```
protocol-control enable
protocol-control disable
```

Parameters

`enable`	Enable lifting L3 control packets to CPU
`disable`	Disable lifting L3 control packets to CPU

Default

By default, Protocol Control is enabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

The below example shows the configuration procedure to enable/disable protocol control for both L2 and L3 interfaces:

L2 Interface:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#protocol-control disable
(config-if)#protocol-control enable
```

L3 Interface:

```
#configure terminal
(config)#interface xe1
(config-if)#protocol-control disable
(config-if)#protocol-control enable
```

show hardware-discard-counters

Use this command to check device level discard counters.

Command Syntax

```
show hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Qumran devices do not support discard counters per interface. Only global level counters are available for advanced debugging using the show hardware-discard-counters command.

Examples

```
#show hardware-discard-counters
+-------------------------------------------------+--------------------+
| Registers                                       | Core 0             |
+-------------------------------------------------+--------------------+
 CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR                     437
   Reason : QNUM_NOT_VALID                         Y
 EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER            8894
   Reason : SRC_EQUAL_DEST_INT                     Y
```

See Table 4-53 and Table 4-54 for details:

Table 4-53: Table detailing about counters supported

Register	Description
CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR for QAX	Drop is due to PPdecision to drop, or invalid destination received from PPblocks.
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER for QMX	The packet DP (Drop Precedence) is higher than the configured Drop DP.
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER	Seen with unknown unicast frames, source and destination learnt from same interface.

Table 4-54: Table detailing about reasons supported

Register	Description
QNUM_NOT_VALID for QAX QUEUE_NOT_VALID_STATUS for QMX	Seen with Vlan Discards, ACL Drops, Storm Control, STP Blocked Port.
DP_LEVEL_RJCT for QAX DP_LEVEL_STATUS for QMX	Seen with Policer Discards.
SRC_EQUAL_DEST_INTF	Seen when traffic is not learned, but is still forwarded/flooded.

show interface

Use this command to display interface configuration and status information.

Command Syntax

```
show interface (IFNAME|)
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1
Interface xe1/1
  Scope: both
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: ecf4.bb6e.934b
  Physical:ecf4.bb6e.934b  Logical:(not set)
  Port Mode is access
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full(auto) link-speed 1g(auto)
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
DHCP client is disabled.
  Last Flapped: 2016 Nov 05 22:40:23 (00:19:25 ago)
  Statistics last cleared: 2016 Nov 05 04:49:55 (18:09:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 39215813 multicast packets 0 broadcast packets 0
    input packets 39215813 bytes 2666662432
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 38902 multicast packets 437 broadcast packets 0
    output packets 437 bytes 28018
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Table 4-55 explains the output fields.

Table 4-55: show interface output details

Field	Description
Scope	Interface can be used for communication within the device and outside the device (Both).
Flexport	Specifies whether the ports has Breakout capabilities or is a Non-Control Port.
Breakout Control Port (Active)	Specifies whether Breakout is active or disabled.
Hardware is ETH Current HW addr	The MAC address of the interface.
Physical	Displays the physical MAC address of the interface.
Logical	Displays the logical MAC address (if any) of the interface.
Port Mode	Displays the port mode: Router, VLAN access, switch, or trunk.
Interface index	Index number, Metric, MTU size, duplex-full (auto) or half-duplex, minimum link speed in gigabits, and if the interface is up, broadcasting, and multicasting.
VRF Binding	Show whether the interface is VRF bound and (if bound) with what VRF, if Label Switching is enabled or disabled, and if a virtual circuit is configured.
DHCP client	The state of the DHCP client – whether this interface is connected to a DHCP server.
Last Flapped	Date and time when the interface last flapped.
Statistics last cleared	Date and time when the interface's statistics were cleared.
5 minute input rate	Input rate in bits/second and packets/second
5 minute output rate	Output rate in bits/second and packets/second
RX	Counters for unicast packets, multicast packets, broadcast packets, input packets, bytes, jumbo packets, runts, giants, CRC errors, fragments, jabbers, input errors, input with dribble input discards, and receive pause.
TX	Counters for unicast packets, multicast packets, broadcast packets, output packets, bytes, jumbo packets, output errors, collisions, differed packets, input late collisions, output discards, and transmit pause.

show interface counters

Use this command to display the ingress and egress traffic counters on the interface.

Note: Counters are meant for debugging purpose and the accuracy of the transmit discard counter is not guaranteed in all scenarios.

Command Syntax

```
show interface (IFNAME|) counters (active|)
show interface cpu counters
```

Parameter

IFNAME	Interface name.
active	Statistics for link-up interfaces.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters
Interface xe1/1
  Scope: both
  Rx Packets: 1000
  Rx Bytes: 1000000
  Rx Unicast Packets: 1000
  Rx Packets from 512 to 1023 bytes: 1000
  Tx Packets: 3897
  Tx Bytes: 249408
  Tx Multicast Packets: 3897
  Tx Packets with 64 bytes: 3897
  Tx Packet rate: 1 pps
  Tx Bit rate: 255 bps

#show interface cpu counters
CPU Interface
  Tx Packets: 104508
  Tx Bytes: 7106272
  Tx Discard Packets: 89613672
  Tx Discard Bytes: 5735237844
  Rx Discard Packets: 11938
```

Table 4-56 explains the output fields.

Table 4-56: show interface counters output details

Field	Description
Receive Counters	Rx Packets Rx Bytes Rx Unicast Packets Rx Multicast Packets Rx Broadcast Packets Rx Packets with 64 bytes Rx Packets from 65 to 127 bytes Rx Packets from 128 to 255 bytes Rx Packets from 256 to 511 bytes Rx Packets from 512 to 1023 bytes Rx Packets from 1024 to 1518 bytes Rx Packets from 1519 to 2047 bytes Rx Packets from 2048 to 4095 bytes Rx Packets from 4096 to 9216 bytes Rx Jumbo Packets Rx Discard Packets (not applicable for Qumran platform) Rx Packets with error Rx CRC Error Packets Rx Undersized Packets Rx Oversized Packets Rx Fragment Packets Rx Jabber Packets Rx MAC error Packets Rx Pause Packets Rx Unrecognized MAC Control Packets Rx Drop Events Rx Packet rate Rx Bit rate

Table 4-56: show interface counters output details

Field	Description
Transmit Counters	Tx Packets Tx Bytes Tx Unicast Packets Tx Multicast Packets Tx Broadcast Packets Tx Packets with 64 bytes Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes Tx Packets from 256 to 511 bytes Tx Packets from 512 to 1023 bytes Tx Packets from 1024 to 1518 bytes Tx Packets from 1519 to 2047 bytes Tx Packets from 2048 to 4095 bytes Tx Packets from 4096 to 9216 bytes Tx Jumbo Packets Tx Discard Packets (not applicable for Qumran platform) Tx Packets with error Tx Collisions Tx Late Collisions Tx Excessive Collisions Tx Pause Packets Tx Packet rate Tx Bit rate
CPU Interface Counters	Tx Packets Tx Bytes Tx Discard Packets Tx Discard Bytes Rx Discard Packets

show interface counters drop-stats

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for physical ports and cpu ports, but not for the out-of-band management (OOB) management port or logical interfaces.

Note: Drops in the CPU queue are listed under `Tx Multicast Queue Drops`, whether the packet is unicast or multicast

Command Syntax

```
show interface (IFNAME|) counters drop-stats
show interface cpu counters drop-stats
```

Parameter

`IFNAME`	Physical interface name
`cpu`	CPU interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.1.

For Qumran devices, only error statistics are applicable and discard counters are not applicable. Only global level counters are available for advanced debugging using the command show hardware-discard-counters.

Example

```
#show interface xe32/2 counters drop-stats
+---------------------+----------------+----------------+--------------------+
| Counter Description | Count          | Last Increment | Last Increment Time
|
+---------------------+----------------+----------------+--------------------+
 Rx Bad CRC errors     0                0
 Rx Undersize errors   0                0
 Rx Oversize errors    0                0
 Rx Fragments errors   0                0
 Rx Jabbers errors     0                0
 Rx Port Block Drops   6                1                2016 Nov 09 08:59:33
 Rx Vlan Discards      0                0
 Rx ACL/QOS Drops      0                0
 Rx Policy Discards    0                0
 Rx EGR Port Unavail   38784            5                2016 Nov 09 18:19:31
 Rx IBP Discards       0                0
 Tx Port Block Drops   359              1                2016 Nov 09 08:59:33
 Tx Vlan Discards      0                0
 Tx TTL Discards       0                0
 Tx Unknown Discards   359              1                2016 Nov 09 08:59:33
 Tx Ucast Queue Drops  0                0
 Tx Mcast Queue Drops  0                0
+---------------------+----------------+----------------+--------------------+
```

Table 4-57 explains the output fields.

Table 4-57: show interface counters drop-stats output details

Field	Description
Counter Description	Shows the type of packet and/or the reason why the packet was dropped.
Count	The number of packets dropped for each reason.
Last Increment	Number of packets dropped since this command was last entered.
Last Increment Time	Date and time when the last packet was dropped.
Rx Bad CRC errors	Received packets dropped because they didn't pass the cyclic Redundancy Check (CRC).
Rx Undersize errors	Number of received runt packets dropped.
Rx Oversize errors	Number of received giant packets dropped
Rx Fragments errors	Number of received packet fragments dropped
Rx Jabbers errors	Received packets dropped because of jabber – long packet error.
Rx Port Block Drops	Received packets dropped because port blocking is enabled (not applicable for Qumran platform).
Rx Vlan Discards	VLAN received packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).
Rx ACL/QOS Drops	Received packets match a field processing entry with a drop or color drop action, such as: User-configured ACL that denies traffic Service policy with a police action that drops the traffic received at a rate higher than the configured limit. (not applicable for Qumran platform)
Rx Policy Discards	Received packets dropped because of device policies violated, such as a storm control rate violation (not applicable for Qumran platform).
Rx EGR Port Unavail	No output port can be determined for these received packets. This counter increments along with other counter types in this table because it is a "catchall" for multiple types of discards as shown below (not applicable for Qumran platform): VLAN check failed MTU check failed ACL/QoS drops Policy discards Source MAC is null Destination IP/source IP address is null Source MAC address and destination MAC address are the same Forwarding lookup failure
Rx IBP Discards	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface. (not applicable for Qumran platform)
Tx Port Block Drops	Transmitted packets dropped because port blocking is enabled (not applicable for Qumran platform).
Tx Vlan Discards	Transmitted VLAN packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).

Table 4-57: show interface counters drop-stats output details (Continued)

Field	Description
Tx TTL Discards	Transmitted packets discarded because their Time To Live (TTL) has ended. (not applicable for Qumran platform)
Tx Unknown Discards	Transmitted packets dropped for unknown reason. May have something to do with the condition/configuration of the port at the other end of the connection (not applicable for Qumran platform).
Tx Ucast Queue Drops	Transmitted packets dropped as a result of Unicast buffer overflow.
Tx Mcast Queue Drops	Transmitted packets dropped as a result of Multicast buffer overflow.

show interface counters error-stats

Use this command to display the ingress error traffic counters on the interface.

Command Syntax

```
show interface (IFNAME|) counters error-stats
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters error-stats
+----------+-------------+--------+----------+---------+-----------+---------+
|Interface |Total errors |Bad CRC |Undersize |Oversize | Fragments | Jabbers |
+----------+-------------+--------+----------+---------+-----------+---------+
 xe1/1      120           8        100        10        2           0
```

Table 4-58 explains the columns in the output.

Table 4-58: error traffic counters

Column	Description	Causes
Interface	Name of the interface	Point of interconnection in network.
Total errors	Total number of all types of errors	Number of errors in network.
Bad CRC	Number of packets received by the port from the network, where the packets have no CRC or a bad CRC.	Packet data modified making the CRC invalid.
Undersize	Total number of packets received that are less than 64 octets long (which exclude framing bits, but include the FCS) and have a good FCS value.	Bad frame generated by the connected device.
Oversize	Number of packets received by the port from the network, where the packets were more than maximum transmission unit size.	Faulty hardware, dot1q, or ISL trunking configuration issues.
Fragments	Total number of frames whose length is less than 64 octets (which exclude framing bits, but which include the FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.
Jabbers	Total number of frames whose length is more than the maximum MTU size. (which exclude framing bits, but which include FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.

show interface counters (indiscard-stats|outdiscard-stats)

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for data ports and CPU ports, not for the out-of-band management (OOB) management port or logical interfaces.

Command Syntax

```
show interface (IFNAME|) counters (indiscard-stats|outdiscard-stats)
show interface cpu counters (indiscard-stats|outdiscard-stats)
```

Parameter

IFNAME	Physical Interface name.
indiscard-stats	Discard reasons for ingress dropped packets.
outdiscard-stats	Discard reasons for egress dropped packets.
cpu	CPU Interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Examples

```
#show interface xe1/3 counters indiscard-stats
+--------------------+----------------+----------------+---------------------+
| Counter Description | Count          | Last Increment | Last Increment Time |
+--------------------+----------------+----------------+---------------------+
 STP Discards          0                0
 Vlan Discards         0                0
 ACL Drops             0                0
 Policy Discards       0                0
 EGR Port Unavail      1092867          1092867          2016 Oct 25 19:54:58
 IBP Discards          0                0
+--------------------+----------------+----------------+---------------------+

#show interface counters indiscard-stats
+-------------+------------------+---------------+---------------+-----------------+------------------+--------------+------
--------------+
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy Discards | EGR Port Unavail | IBP Discards |   Total
Discards   |
+-------------+------------------+---------------+---------------+-----------------+------------------+--------------+------
--------------+
xe1           0                  0               35703           0                 11                 0              35714
xe2           0                  0               295744          0                 13604              0              309348
xe3           0                  0               9501            0                 20405              0              29906
xe5           0                  0               0               0                 13602              0              13602
xe49/1        0                  0               0               0                 0                  20658          20658
xe52/1        0                  3               856029          10                13613              0              869642
xe54/1        0                  5371            0               0                 5371               0              5371
cpu           0                  0               0               0                 6                  0              N/A

#show interface counters outdiscard-stats
```

```
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
-------------+
|  Interface  | Port Block Drops | Vlan Discards | TTL Discards | Unknown Discards |  UcastQ Drops  |  McastQ Drops  |   Total
Discards   |
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
-------------+
xe1           0                 0              0             204338            0               0               204338
xe2           0                 0              0             1094368           0               0               1094368
xe3           0                 0              0             818672            0               0               818672
xe52/1        0                 0              0             1275156           0               0               1275156
xe54/1        0                 0              0             13575             0               0               13575
cpu           0                 0              0             0                 N/A             1014224         N/A
```

Table 4-59 explain the fields in the command output.

Table 4-59: indiscard statistic output details

Statistic	Description
STP Discards	Packets received when the ingress interface is not in STP forwarding state.
Port Block Drops	Packets discarded on an ingress interface where port blocking is configured.
VLAN Discards	VLAN tagged packets received on a port which is not a member of the VLAN or untagged packets received on a trunk port.
ACL/QoS Drops	Incoming packets match a field processing entry with a drop or color drop action, such as: 1. User-configured ACL that denies traffic 2. Service policy with a police action that drops the traffic received at a rate higher than the configured limit
Policy Discards	Device policies violated, such as a storm control rate violation, source or destination discards when L2 tagged traffic received on router interface.
EGR (Egress) Port Unavail	No output port can be determined for this packet. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below: 1. VLAN check failed 2. MTU check failed 3. ACL/QoS drops 4. Policy discards 5. Source MAC is null 6. Destination IP/source IP address is null 7. Source MAC address and destination MAC address are the same 8. Source MAC is configured as static on other interface 9. Forwarding lookup failure
IBP Drops	Ingress Back Pressure (ingress congestion) when the ingress packet buffer is full for an interface.
Total Discards	Total number of ingress dropped packets.

Table 4-60 explain the fields in the command output.

Table 4-60: outdiscard statistics

Statistics	Description
Port Block Drops	Packets discarded on an egress interface where port blocking is configured.
VLAN Discards	Packets discarded because an invalid VLAN tag is encountered at an egress interface.
TTL Discards	Packets discarded because the Time-To Live (TTL) of the outgoing packet has passed.

Table 4-60: outdiscard statistics

Statistics	Description
Unknown Discards	Packets discarded for other possible reasons like ACL drop in egress or a policer drop in egress. Discards caused by congestion at queues and drops at queues are not counted under unknown discards.
Unicast Queue Drops	Packets dropped in the unicast queues because of congestion.
Multicast Queue Drops	Packets dropped in the multicast queues because of congestion.
Total Discards	Total number of egress dropped packets.

show interface counters protocol

Use this command to display protocol packets received at the CPU by the control plane.

Command Syntax

```
show interface (IFNAME|) counters protocol
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
#show interface counters protocol
Interface ce1/1
  lacp                : 4
  icmp6               : 5
```

Table 4-61 explain the fields in the command output.

Table 4-61: show interface counters protocol output details

Field	Description
Interface	Name of the configured interface.
lacp	Total number of lacp protocol in the interface.
icmp6	Total number of icmp6 protocol in the interface.

show interface counters queue-drop-stats

Use this command to display dropped packets in the CPU queue and the last increment time.

Command Syntax

```
show interface cpu counters queue-drop-stats
```

Parameters

cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
show interface cpu counters queue-drop-stats
+------------------+---------------+----------------+---------------------+
|    Queue Name    |     Count     | Last Increment | Last Increment Time |
+------------------+---------------+----------------+---------------------+
arp                  169735545        9145653          2017 Oct 23 14:33:54
```

Table 4-62 explain the fields in the command output.

Table 4-62: show interface counters queue-drop-stats output details

Field	Description
Queue Name	Name of the protocol.
Count	Number of arp protocols in the interface.
Last Increment	Final increment number in the protocol.
Last Increment time	Time of the last increment in the protocol.

show interface counters queue-stats

Use this command to display transmitted and dropped packet and byte counts of individual queues.

Note: In Qumran devices, all packets dropped in a queue are counted (even policer drops).

Command Syntax

```
show interface (IFNAME|) counters queue-stats
show interface cpu counters queue-stats
```

Parameters

IFNAME	Interface name.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Note: Default traffic counters are not supported on Qumran AX.

Example

```
#show interface counters queue-stats
D - Default Queue, U - User-defined Queue
+--------+---------------+------+-----------+------------+------------+---------------+
|Interface|Queue/Class-map|Q-Size|Output pkts|Output bytes|Dropped pkts|Dropped bytes  |
+--------+---------------+------+-----------+------------+------------+---------------+
xe1/1     q1          (D) 0      12          1368         0            0
xe1/1     mc-q7       (D) 0      1           82           0            0
xe25      q1          (D) 0      6           684          0            0

#show interface xe1/1 counters queue-stats
D - Default Queue, U - User-defined Queue
+---------------+------+-------+-  -------+------------+--------------+
|Queue/Class-map|Q-Size|Tx pkts| Tx bytes |Dropped pkts|Dropped bytes |
+---------------+------+-------+----------+------------+--------------+
q0            (D) 0     0       0          0            0
q1            (D) 0     12      1368       0            0
q2            (D) 0     0       0          0            0
q3            (D) 0     0       0          0            0
q4            (D) 0     0       0          0            0
q5            (D) 0     0       0          0            0
q6            (D) 0     0       0          0            0
q7            (D) 0     0       0          0            0
mc-q0         (D) 0     0       0          0            0
mc-q1         (D) 0     0       0          0            0
mc-q2         (D) 0     0       0          0            0
mc-q3         (D) 0     0       0          0            0
mc-q4         (D) 0     0       0          0            0
mc-q5         (D) 0     0       0          0            0
mc-q6         (D) 0     0       0          0            0
mc-q7         (D) 0     1       82         0            0

#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |   Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
igmp              (E) 800592   14519             987292              1304163           88683084
```

```
arp             (E) 1250496  1008785          68597380          0               0
```

Table 4-63 explain the fields in the command output.

Table 4-63: queue flags detail

Flag	Meaning
D	Default queue of the port.
U	User defined queue of the port.
E	Outgoing hello packet's queue in the port.
I	Incoming hello packet's queue in the port.
Q	Hello packet's queue size in bytes.

Table 4-64 explain the fields in the command output.

Table 4-64: show interface counters queue-stats output details

Field	Description
Interface	A defined physical interface to which the queue is associated.
Queue/Class-map	Queues associated with a QoS class-map.
Q-Size	The size of a specified queue in bytes.
Output pkts	The number of out bound packets residing in the queues.
Output Bytes	The number of bytes in the outbound queue.
Dropped pkts	The number of packets dropped because of queue overflow.
Dropped bytes	The number of bytes dropped because of queue overflow.
Tx pkts	The number of transmit packets contained in the out bound queue.
Tx bytes	The number of transmit bytes contained in the out bound queue.

show interface counters rate

Use this command to display the average traffic rate over the load interval of the interface.

Command Syntax

```
show interface (IFNAME|) counters rate (kbps|mbps|gbps|)
show interface cpu counters rate (kbps|mbps|gbps|)
```

Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface counters rate
+-------------+---------------------------+--------------------------------+
|             |              Rx           |               Tx               |
|  Interface  |---------------------------+--------------------------------|
|             |      bps     |      pps   |      bps      |      pps       |
+-------------+---------------------------+--------------------------------+
 xe1/1         548439552       1008160     544400           1000

#show interface cpu counters rate
Load interval: 30 second
+------------------+--------------+-------------+--------------+-------------+
|    CPU Queue(%)  |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps   |
+------------------+--------------+-------------+--------------+-------------+
 isis         (  0%) -              -             742            0
 arp          (  0%) -              -             6              0
```

Table 4-65 explain the fields in the command output.

Table 4-65: show interface counters rate output details

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
CPU Queue	CPU Queues used for various functions. In the example the CPU is maintaining queues for ARP and the IS-IS routing facilities.
Load interval	The length of time for which data is used to compute load statistics.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

show interface counters speed

Use this command to display the current average speed on the interface.

Command Syntax

```
show interface (IFNAME|) counters speed (kbps|mbps|gbps|)
```

Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show interface counters speed
* indicates monitor is active
+------------+--------------+--------------------+---------------------------
---------------+
|            |              |     Threshold(%)   |          Current average
speed           |
|  interface | configured   +--------------------+-------------+-------+------
-------+-------+
|            | speed ( bps) | Warning | Recovery |  Rx ( bps)  |   %   |  Tx (
bps)  |   %   |
+------------+--------------+---------+----------+-------------+-------+------
-------+-------+
  ce45       100000000000   90        80         0            0.00    0
0.00
  xe7        10000000000    90        80         0            0.00    0
0.00
  xe31       10000000000    90        80         0            0.00    0
0.00
  xe33       10000000000    90        80         0            0.00    0
0.00
  xe39       10000000000    90        80         0            0.00    0
0.00
  xe40       10000000000    90        80         0            0.00    0
0.00
#
```

show interface counters summary

Use this command to display the summary of traffic counters on a specific interface or all interfaces.

Note: This command is supported for the out-of-band management (OOB) management interface.

Command Syntax

```
show interface (IFNAME|) counters summary
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters summary
+-----------+------------------------------+------------------------------+
|           |              Rx              |              Tx              |
| Interface |------------------------------+------------------------------|
|           |    packets    |     bytes    |    packets    |     bytes    |
+-----------+---------------+--------------+---------------+--------------+
 xe1/1       11032977        11032960000     61              3904


#show interface counters summary
+-------------+--------------------+--------------------+--------------------+--------------------+
|  Interface  |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes      |
+-------------+--------------------+--------------------+--------------------+--------------------+
 eth0          206222               13756391             235123               337010937
 po1           809121               72989094             825221               90605534
 xe1/1         0                    0                    1                    114
 xe3/1         43                   4730                 21                   2298
 xe5/1         29                   3178                 21                   2298
 xe8           10                   1076                 14                   1532
 xe9/1         16                   1760                 21                   2298
 xe11/1        0                    0                    7                    766
 xe19/1        12426292             1298526692           6                    620
 xe21/1        13                   1386                 14                   1532
 xe28/1        3144                 202370               21                   2298
 xe30/1        3161                 202304               7                    766
 xe32/1        694067               61687838             710274               79315093
 xe32/2        115054               11301256             114947               11290441
 xe32/3        603759               51208946             620502               68865557
 xe32/4        7                    766                  7                    766
```

Table 4-66 explain the fields in the command output.

Table 4-66: show interface counters summary output details

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

show interface protocol-control status

Use this command to display the interfaces on which protocol-control is disabled.

Command Syntax

```
show interface protocol-control status
```

Parameter

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show interface protocol-control status
Interfaces for which ARP/DHCP/ND Pkts will not be forwarded to CPU
Interface
---------
xe20
```

show ip forwarding

Use this command to display the IP forwarding status.

Command Syntax

```
show ip forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on
#
```

Table 4-67 explain the fields in the command output.

Table 4-67: show ip forwarding

Field	Description
vrf (management)	Management VRF is for management purposes. IP forwarding packet is on.
vrf (default)	The default VRF uses the default routing context for ip forwarding. IP forwarding packet is on.

show ip interface

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ip interface brief
show ip interface IFNAME brief
```

Parameters

`IFNAME`	Interface name.
`brief`	Brief summary of IP status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
eth0                *10.10.26.101    up                    up
lo                   127.0.0.1       up                    up
lo.management        127.0.0.1       up                    up
xe1/1                10.1.1.1        up                    up
xe1/2                unassigned      down                  down
xe1/3                unassigned      down                  down
xe1/4                unassigned      down                  down
xe2                  unassigned      up                    down
xe3/1                unassigned      up                    up
xe3/2                unassigned      down                  down
xe3/3                unassigned      down                  down
```

Table 4-68 explain the fields in the command output.

Table 4-68: show ip interface output details

Field	Description
Interface	Interface name, also specifies interface type (eth0, lo, xe1/1, and xe1/2).
IP-Address	The IP address assigned to the interface. An asterisks indicates that the IP address was provided by DHCP.

Table 4-68: show ip interface output details (Continued)

Field	Description
Admin-Status	Interface is up and functioning or down.
Link-Status	Interface is connected and passing traffic.

show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

Syntax Description

```
show ip prefix-list
show ip prefix-list WORD
show ip prefix-list WORD seq <1-4294967295>
show ip prefix-list WORD A.B.C.D/M
show ip prefix-list WORD A.B.C.D/M longer
show ip prefix-list WORD A.B.C.D/M first-match
show ip prefix-list summary
show ip prefix-list summary WORD
show ip prefix-list detail
show ip prefix-list detail WORD
```

Parameters

`WORD`	Name of a prefix list.
`A.B.C.D/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Lookup longer prefix.
`<1-4294967295>`	Sequence number.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display all routes (selected and not selected), use the `show ip route database` command.

Command Syntax

```
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route (database|)
show ip route (database|) (bgp|connected|database|isis|fast-
  reroute|interface|isis|kernel|mbgp|mstatic|next-hop|ospf|rip|static)
show ip route summary
show ip route vrf WORD (database|)
show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
```

Parameters

`A.B.C.D`	Network in the IP routing table.
`A.B.C.D/M`	IP prefix <network>/<length>, for example, 35.0.0.0/8.
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	Routing table database.
`fast-reroute`	Fast reroute repair paths.
`interface`	Interface.
`isis`	IS-IS.
`kernel`	Kernel.
`mbgp`	Multiprotocol BGP routes.
`mstatic`	Multicast static routes.
`next-hop`	Next hop address.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes.
`WORD`	Routes for a Virtual Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: Display FIB Routes

The following shows output for the best routes.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
Gateway of last resort is 10.30.0.11 to network 0.0.0.0

K*      0.0.0.0/0 via 10.30.0.11, eth0
O       9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:18:56
K       10.10.0.0/24 via 10.30.0.11, eth0
C       10.10.31.0/24 is directly connected, eth2
S       10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
C       10.30.0.0/24 is directly connected, eth0
S       11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
S       16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O       17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:20:54
C       45.45.45.45/32 is directly connected, lo
O       55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:20:54
C       127.0.0.0/8 is directly connected, lo
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route and K indicates that the route has been learned from the kernel. Table 4-69 shows these codes and modifiers.

Table 4-69 explain the fields in the command output.

Table 4-69: route codes and modifiers

Code	Meaning	Description
K	kernel	Routes added through means other than by using the CLI; for example by using the operating system route command. Static routes added using kernel commands and static routes added using OcNOS commands are different. The kernel static routes are not redistributed when you give the `redistribute static` command in a protocol. However, the kernel static routes can be redistributed using the `redistribute kernel` command.
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols. Routes for connected networks always exist in the kernel routing table but as an exception are not marked as kernel routes because OcNOS always calculates entries for these routes upon learning interface information from the kernel.
S	static	Routes manually configured via CLI which are not updated dynamically by IGPs.
The codes below are for routes received and dynamically learned via IGP neighbors. These networks are not directly connected to this device and were announced by some other device on the network. IGPs update these routes as the network topology changes.		
R	RIP	RIP routing process and enter Router mode.
B	BGP	Route is from an Border Gateway Protocol.
O	OSPF	Modifiers for OSPF: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
i	IS-IS	Modifiers for IS-IS: L1 - IS-IS level-1 L2 - IS-IS level-2 ia - IS-IS inter area
Other modifiers:		
v	vrf leaked	The device has two or more VRFs configured and each has at least one interface bound to it. While each VRF will have its own routing table, the VRFs can learn each other's routes.
*	candidate default	Route has been added to the FIB. With equal cost paths to a destination, the router does per-packet or per-destination load sharing. An asterisk ("*") means that the route is being used at that instant for forwarding packets. If you run the same `show ip route x.x.x.x` command over and over, you might see the * moving between the route entries.
>	selected route	When multiple routes are available for the same prefix, the best route. When multiple entries are available for the same prefix, OcNOS uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. OcNOS populates the FIB with the *best* route to each destination
p	stale info	A route information that is marked stale due to graceful restart.

After the codes, the header has default gateway information:

```
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```

The “gateway of last resort”, also called the default gateway, is a static route that routes IP address 0.0.0.0 (all destinations) through a single host (the gateway). The effect of setting a gateway is that if no routing table entry exists for a destination address, packets to that address will be forwarded to the gateway router.

Route Entry Fields

Table 4-70 explains the each route entry fields.

Table 4-70: route entry output details

Field	Description
Codes and modifiers	As explained in Table 4-69.
IP address	IP address of the remote network.
Administrative distance and metric	The administrative distance determines how trustworthy this route is. If there is a similar route but with a smaller administrative distance, it is used instead, because it is more “trustworthy”. The smaller the administrative distance, the more trustworthy the route. Directly connected routes have an administrative distance of 0, which makes them the most trustworthy type of route.The metric varies from protocol to protocol, and for OSPF the metric is cost, which indicates the best quality path to use to forward packets. Other protocols, like RIP, use hop count as a metric. For neighboring routers, the metric value is 1.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Duration	Length of time that this route has been present in the routing table. This is also the length of time this route has existed without an update. If the route were removed and then re-added (if the cable was disconnected, for instance), this timer would begin again at 00:00:00.

Route Entry Examples

```
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
```

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via nexthop 10.10.31.16.
- The outgoing local interface for this route is eth2.
- This route was added 20 minutes and 54 seconds ago.

```
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
```

- This route is the same as the other OSPF route above; the only difference is that it is a Type 2 External OSPF route.

```
C       10.10.31.0/24 is directly connected, eth2
```

- This route is directly connected.
- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth2.

```
K       10.10.0.0/24 via 10.30.0.11, eth0
```

- This route in the network 10.10.0.0/24 was learned from the kernel routing table (route was statically added using kernel commands).

- This route is reachable via nexthop 10.30.0.11.
- The outgoing local interface for this route is eth0.

```
K*      0.0.0.0/0 via 10.30.0.11, eth0
```

- This is a default route that was learned from the kernel (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The local interface for this route is eth0.

Example: Display OSPF Routes

The following is the output with the `ospf` parameter:

```
#show ip route ospf
O       1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:44
O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:44
#
```

Example: Display Route Summary

The following is the output with the `summary` parameter.

```
#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source    Networks
kernel          1
connected       5
ospf            2
Total           8
FIB             2
```

Example: Display RIB Routes

The following shows displaying database routes.

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

K    *> 0.0.0.0/0 via 10.30.0.11, eth0
O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:19:21
K    *> 10.10.0.0/24 via 10.30.0.11, eth0
O       10.10.31.0/24 [110/1] is directly connected, eth2, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:21:19
K    *  10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:19:21
O       16.16.16.16/32 [110/11] via 10.10.31.16, eth2, 00:21:19
```

```
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:21:19
K    *  127.0.0.0/8 is directly connected, lo
C    *> 127.0.0.0/8 is directly connected, lo
```

The codes and modifier at the start of each route entry are explained in Table 4-69.

Routes in the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. Unselected routes have neither the * nor the > symbol.

Route Database Entry Examples

This example shows 2 entries in the route database; one learned from the kernel and the other derived from interface information.

```
K    * 10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
```

- Both these routes are in the same network 10.30.0.0/24.
- The first route has originated from the kernel. The * indicates that it has been added to the FIB.
- The second route is derived from the IP address of local interface eth0. It is marked as a connected route. Since a connected route has the lowest administrative distance, it is the selected route.

```
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O      10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
```

- The same prefix was learned from OSPF and from static route configuration.
- Static routes are preferred over OSPF routes, so the static route is selected and installed in the FIB.

  Note: If the static route becomes unavailable, OcNOS automatically selects the OSPF route and installs it in the FIB.

Example: Display VRF Routes

The following is the output with the `vrf` parameter:

```
#show ip route vrf vrf31
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
* - candidate default

IP Route Table for VRF "vrf31"
O            2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
C            21.1.1.0/24 is directly connected, vlan1.4, 00:02:54
C            31.31.1.1/32 is directly connected, lo.vrf31, 00:03:02
O            40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:43
C            127.0.0.0/8 is directly connected, lo.vrf31, 00:03:05

Gateway of last resort is not set
```

The following is the output with the `vrf database` parameter:

```
#show ip route vrf vrf31 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf31"
O    *>  2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
C    *>  21.1.1.0/24 is directly connected, vlan1.4, 00:02:57
O        21.1.1.0/24 [110/1] is directly connected, vlan1.4, 00:02:57
C    *>  31.31.1.1/32 is directly connected, lo.vrf31, 00:03:05
O        31.31.1.1/32 [110/1] is directly connected, lo.vrf31, 00:03:00
O    *>  40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:46
B     >  50.1.1.0/24 [200/0] via 41.41.41.41, 00:00:18
C    *>  127.0.0.0/8 is directly connected, lo.vrf31, 00:03:08

Gateway of last resort is not set
```

show ip vrf

This command displays routing information about VRFs.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	Virtual Routing and Forwarding name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip forwarding
 vrf (management) :IP forwarding is on
 vrf (default) :IP forwarding is on
```

show ipv6 forwarding

Use this command to display the IPv6 forwarding status.

Command Syntax

```
show ipv6 forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
 vrf (management) :IPv6 forwarding is on
 vrf (default) :IPv6 forwarding is on#
```

show ipv6 interface brief

Use this command to display information about interfaces. To display information about a specific interface, include the interface name.

Command Syntax

```
show ipv6 interface brief
show ipv6 interface IFNAME brief
```

Parameters

IFNAME	Name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 interface brief
Interface           IPv6-Address                Admin-Status
lo                  ::1                         [up/up]

gre0                unassigned                  [admin down/down]

eth3                3ffe:abcd:104::1            [up/up]
                    3ffe:abcd:103::1
                    fe80::2e0:29ff:fe6f:cf0

eth1                fe80::260:97ff:fe20:f257    [up/up]

eth2                unassigned                  [admin down/down]

eth3                unassigned                  [admin down/down]

sit0                unassigned                  [admin down/down]

tun24               unassigned                  [admin down/down]

tunl0               unassigned                  [admin down/down]
```

Table 4-71 explains the each interface brief entry.

Table 4-71: show interface brief output details

Field	Description
Interface	Name of the interface.
IPv6-Address	IPv6 address. An asterisk (“*”) means the address was assigned by the DHCPv6 client.
Admin-Status	Status of the interface: The first part of the field indicates if the interface is up. The second part indicates if the interface is running.

show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes in the FIB can be viewed using `show ipv6 route`.

Command Syntax

```
show ipv6 route vrf WORD (database|)
show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route (database)
show ipv6 route (database) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route X:X::X:X
show ipv6 route X:X::X:X/M
show ipv6 route summary
```

Parameters

`X:X::X:X`	Network in the IP routing table.
`X:X::X:X/M`	Prefix <network>/<length>, e.g., 35.0.0.0/8
`all`	All IPv6 routes
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	IPv6 routing table database.
`isis`	IS-IS.
`IFNAME`	Interface name
`kernel`	Kernel.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes
`WORD`	Routes from a Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

See Table 4-69 and Table 4-70 for an explanation of the codes and fields in the output.

```
#show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
```

```
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.
C> * ::1/128 is directly connected, lo
C> * 3ffe:1::/48 is directly connected, eth1
C> * 3ffe:2:2::/48 is directly connected, eth2
#
```

show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

Syntax Description

```
show ipv6 prefix-list
show ipv6 prefix-list WORD
show ipv6 prefix-list WORD seq <1-4294967295>
show ipv6 prefix-list WORD X:X::X:X/M
show ipv6 prefix-list WORD X:X::X:X/M longer
show ipv6 prefix-list WORD X:X::X:X/M first-match
show ipv6 prefix-list summary
show ipv6 prefix-list summary WORD
show ipv6 prefix-list detail
show ipv6 prefix-list detail WORD
```

Parameters

`WORD`	Name of prefix list.
`X:X::X:X/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Look up longer prefix.
`<1-4294967295>`	Sequence number of an entry.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

show hosts

Use this command to display the IP domain-name, lookup style and any name server.

Command Syntax

```
show hosts
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show hosts

       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 4-72 explains the output fields.

Table 4-72: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF
DNS lookup is enabled	DNS feature enabled or disabled
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 4-72: show hosts fields

Entry	Description
Host Address test 10.12.12.67 test 10::23	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	* in name-server indicates it has been learned dynamically.

show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

Command Syntax

```
show running-config interface IFNAME
show running-config interface IFNAME bridge
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 rip
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME isis
show running-config interface IFNAME lacp
show running-config interface IFNAME ldp
show running-config interface IFNAME mpls
show running-config interface IFNAME mstp
show running-config interface IFNAME ospf
show running-config interface IFNAME ptp
show running-config interface IFNAME rip
show running-config interface IFNAME rstp
show running-config interface IFNAME rsvp
show running-config interface IFNAME stp
show running-config interface IFNAME synce
```

Parameters

`bridge`	Bridge.
`ip`	IPv4 (see also show running-config interface ip).
`ipv6`	IPv6 (see also show running-config interface ipv6).
`isis`	Intermediate System to Intermediate System.
`lacp`	Link Aggregation Control Protocol.
`ldp`	Label Distribution Protocol.
`mpls`	Multi-Protocol Label Switching.
`mstp`	Multiple Spanning Tree Protocol.
`ospf`	Open Shortest Path First.
`ptp`	Precision Time Protocol.
`rip`	Routing Information Protocol.

`rstp`	Rapid Spanning Tree Protocol.
`rsvp`	Resource Reservation Protocol.
`stp`	Spanning Tree Protocol.
`synce`	Synchronous Ethernet.

Command Mode

Privileged Exec mode and Config Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 bridge
!
interface eth1
 switchport
 bridge-group 1
 switchport mode access
 user-priority 3
 traffic-class-table user-priority 2 num-traffic-classes 3 value 3 traffic-
class-table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table
user-priority 7 num-traffic-classes 2 value 0 traffic-class-table user-
priority 7 num-traffic-classes 3 value 0 traffic-class-table user-priority 7
num-traffic-classes 4 value 0 traffic-class-table user-priority 7 num-traffic-
classes 5 value 0 traffic-class-table user-priority 7 num-traffic-classes 6
```

show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

Command Syntax

```
show running-config interface IFNAME ip (igmp|multicast|pim|)
```

Parameters

`IFNAME`	Interface name.
`igmp`	Internet Group Management Protocol.
`multicast`	Multicast.
`pim`	Protocol Independent Multicast.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
 switchport
```

show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

Command Syntax

```
show running-config interface IFNAME ipv6 (mld|multicast|ospf|pim|rip|)
```

Parameters

`IFNAME`	Interface name.
`mld`	Multicast Listener Discovery
`multicast`	Multicast
`ospf`	Open Shortest Path First
`pim`	Protocol Independent Multicast
`rip`	Routing Information Protocol

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ipv6 rip
!
interface eth1
 switchport
```

show running-config ip

Use this command to show the running system of IP configurations.

Command Syntax

```
show running-config ip (dhcp|mroute|route)
```

Parameters

`dhcp`	Dynamic Host Configuration Protocol.
`mroute`	Static IP multicast route.
`route`	Static IP route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ip route
!
ip route 3.3.3.3/32 eth3
ip route 3.3.3.3/32 eth2
ip route 200.0.0.0/16 lo
!
```

show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

Command Syntax

```
show running-config ipv6 (access-list|mroute|neighbor|prefix-list|route|)
```

Parameters

`access-list`	Access list.
`mroute`	Static IPv6 Multicast route.
`neighbor`	Static IPv6 neighbor entry.
`prefix-list`	IPv6 prefix-list.
`route`	Static IPv6 route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 eth2
ipv6 route fe80::/64 eth2
!
```

shutdown

Use this command to shut down an interface.

Use the no form of this command to bring up an interface.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth3`.

```
#configure terminal
(config)#interface eth3
(config-if)#shutdown
```

speed

Use this command to set the link speed of the interface.

Use the no parameter to set the speed to its default value.

On copper ports, auto-negotiation is enabled by default and force speed is not supported.

On fiber optic ports, auto-negotiation is disabled by default. Auto-negotiation is not supported on fiber optic medium/ AOC for speeds 10g and beyond. IP Infusion Inc.does not recommend using auto speed on such transceivers. On DAC cables, both force and auto-negotiation are supported.

IP Infusion Inc. recommends configuring the same speed mode on both peers.

When an interface is configured with the speed auto option:

- The negotiated parameters are speed, duplex, flowcontrol, and fec, each of which is configured separately. Please see the respective command for details.
- If the speed of the optic connected is less than the front-panel port capability, then the interface does not come up in auto mode. To bring up the interface, use the `speed auto <speed>` command to reduce the negotiation capability. For example, if the front panel port is 10g capable and in auto mode and you insert a 1g SFP, then the hardware tries to bring up port in 10g and fails. Use the command `speed auto 1g` to start the negotiation at the 1g speed and the port will come up.

Note: For 10g DAC/AOC, setting speed auto negotiates with a maximum of 1G.

Table 4-73 shows the IP Infusion Inc. recommendations regarding front-panel port speed and transceivers.

Table 4-73: Recommendatons

Suported/ Recommended	Explanation
Not Supported	When front panel port capability is less than the transceiver's capability the behavior is undefined.
Not Recommended	When the transceiver's capability and front panel port capability is the same, reducing the speed is not recommended.
Recommended	When the transceiver's capability is less than the front panel port capability, the behavior is undefined and the link might even come up. So speed needs to be set to match the transceiver's capability.

Table 4-74 show examples with front-panel configurations:

Table 4-74: Front-panel configurations

Front Panel Port	Explanation
Front Panel Port 100g	When 40g transceivers are used, make sure to use the command `speed 40g`. IP Infusion Inc. does not recommend using 40g on 100g speed transceivers.
Front Panel Port 40g	100g transceivers should not be used.

Table 4-74: Front-panel configurations (Continued)

Front Panel Port	Explanation
Front Panel Port 25g	When 10g transceivers are used, make sure to use the `port-group` command to reduce the speed to 10g. IP Infusion Inc. does not recommend to use 10g on 25g speed transceivers. When using 1g transceivers, make sure to set the speed to 1g. Below 25g, port-speed can defer (10g or 1g) for ports under same port-group i.e. 1 port can have 1g & remaining 10g but 1 port 25g & remaining 10g not allowed. When "`no speed`" command is used at interface level it tries to set speed "25g" to one of the port of port-group while other may be at 10g or 1g speed which is not allowed. Use "`no port-group`" command in such case.
Front Panel Port 10g	25g transceivers should not be used. When using 1g transceivers, make sure to set the speed to 1g.
Front Panel Port 1g	10g/25g transceivers should not be used.

Command Syntax

```
speed (10m | 100m | 1g | 2.5g | 10g | 20g | 25g | 40g | 50g | 100g |
  (auto (1g | 10g | 20g | 25g | 40g | 50g | 100g |)))
no speed
```

Parameter

`10m`	10 megabits
`100m`	100 megabits
`1g`	1 gigabit
`2.5g`	2.5 gigabits
`10g`	10 gigabits
`20g`	20 gigabits
`25g`	25 gigabits
`40g`	40 gigabits
`50g`	50 gigabits
`100g`	100 gigabits
`auto`	Negotiate the speed with a connected port

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Enable auto-negotiation up to 1G:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto 1g
```

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured `routed` by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

User should be prompted for confirmation, while executing `switchport/no switchport` command. To support this requirement, please refer the command `enable/disable confirmation-dialog.`

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no switchport
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport

#configure terminal
(config)#enable confirmation-dialog
(config)#interface xe5
(config-if)#switchport
Are you sure? (y/n): y
(config-if)#
(config-if)#exit

(config)#disable confirmation-dialog
(config)#
(config)#interface xe5
(config-if)#switchport
(config-if)#
```

switchport allowed ethertype

Use this command to indicate which types of traffic will be allowed on the switchport.

Note: A maximum of 5 Ethertype values can be assigned on an interface.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|ETHTYPE|log}
```

Parameters

`arp`	ARP traffic
`ipv4`	IPv4 traffic
`ipv6`	IPv6 traffic
`mpls`	MPLS traffic
`ETHTYPE`	Traffic of any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```

CHAPTER 5 Access Control List Commands

This chapter is a reference for the Access Control List (ACL) commands:

- mac access-list remark
- mac access-list resequence
- show access-lists
- show arp access-lists
- show ip access-lists
- show ipv6 access-lists
- show mac access-lists
- show running-config access-list
- show running-config aclmgr
- show running-config ipv6 access-list

arp access-group

Use this command to attach an ARP access list to an interface to filter incoming ARP packets.

When you attach an ARP access list to a LAG interface as well as to a physical interface that is a member of that LAG interface, the priority order is:

1. LAG interface
2. Physical interface

Use the `no` form of this command to detach an ARP access group.

Note: An ARP access-list is supported only on switch ports.

Note: To attach an ARP access-group to an interface, the `ingress-arp` TCAM group should be enabled. See the hardware-profile filter command for details.

Command Syntax

```
arp access-group NAME in
no arp access-group NAME in
```

Parameters

`NAME`	ARP access list name

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#permit ip any mac any
(config-arp-acl)#exit

(config)#interface xe1
(config-if)#arp access-group arp1 in
(config-if)#exit

(config)#interface xe1
(config-if)#no arp access-group arp1 in
(config-if)#exit
```

arp access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop the ARP packets, based on the ARP request or response option configured.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. A single-entry ACL with only one deny specification is the same as denying all traffic. You must have at least one permit specification in an ACL or all traffic is blocked.

Use the no form of this command to remove an ACL specification.

Note: An ARP access list is supported only on switch ports.

Command Syntax

```
arp access-list NAME
no arp access-list NAME
```

Parameters

NAME	ARP access list name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#arp access-list arp1
```

arp access-list default

Use this command to modify the default rule action of an access list.

The default rule is applicable only when an access list is attached to an interface. The default rule will have the lowest priority and only ARP packets not matching any of the user defined rules match the default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

The default rule is `deny-all` when an access list is attached to an interface.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#default permit-all
```

arp access-list remark

Use this command to add a description to a named ARP access control list (ACL).

Use the no form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

LINE	ACL description up to 100 characters.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)# remark Permit arp request packets
```

arp access-list request

Use this command to configure ARP access control entry in an ARP access control list (ACL).

This command determines whether to accept or drop a packet based on the configured match criteria.

Use the no form of this command to remove an ACL specification.

Note: Configuring the same filter again with a change of sequence number or change of action will result in updating the sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit)(request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | ((XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
  (XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | ((XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
  (XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (vlan <1-4094>|) (inner-vlan <1-4094>|)
```

Parameters

<1-268435453>	ARP ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
request	ARP request.
ip	Internet Protocol (IP).
A.B.C.D/M	Source IP prefix and length.
A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.
mac	MAC address configuration.
any	Match any source mac address.
XX-XX-XX-XX-XX-XX	Source MAC address (Option 1).
XX:XX:XX:XX:XX:XX	Source MAC address (Option 2).
XXXX.XXXX.XXXX	Source MAC address (Option 3).
XX-XX-XX-XX-XX-XX	Source wildcard (Option 1).
XX:XX:XX:XX:XX:XX	Source wildcard (Option 2).
XXXX.XXXX.XXXX	

Source wildcard (Option 3).

`host (XX-XX-XX-XX-XX-XX)`

A single source host MAC address.

`vlan <1-4094>` VLAN identifier.

`inner-vlan <1-4094>`

Inner VLAN identifier.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#10 permit request ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
(config-arp-acl)#no 10
```

arp access-list resequence

Use this command to modify the sequence numbers of an ARP access list.

Note: IP Infusion Inc. recommends to use a non-overlapping sequence space for a new sequence number set to avoid unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#resequence 15 15
```

arp access-list response

Use this command to configure an ARP access control entry in an ARP access control list (ACL).

This command determines whether to accept or drop an ARP response packet based on the configured match criteria.

Use the no form of this command to remove an ACL specification.

Note: Configuring the same filter again with a change of sequence number or change of action will result in updating the sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | ((XX-XX-XX-
  XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) -XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (any | ((XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)))(vlan <1-4094>|) (inner-vlan <1-4094>|)

no (<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | ((XX-XX-XX-
  XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) -XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (any | ((XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)))(vlan <1-4094>|) (inner-vlan <1-4094>|)
```

Parameters

<1-268435453>	ARP ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
response	ARP response
A.B.C.D/M	Source/destination IP prefix and length.
A.B.C.D A.B.C.D	Source/destination IP address and mask.
host A.B.C.D	A single source/destination host IP address.
any	Match any source/destination IP address.
mac	MAC address configuration.
any	Match any source/destination MAC address.
XX-XX-XX-XX-XX-XX	Source/destination MAC address (Option 1).
XX:XX:XX:XX:XX:XX	Source/destination MAC address (Option 2).
XXXX.XXXX.XXXX	Source/destination MAC address (Option 3).

`XX-XX-XX-XX-XX-XX`
: Source/destination wildcard (Option 1).

`XX:XX:XX:XX:XX:XX`
: Source/destination wildcard (Option 2).

`XXXX.XXXX.XXXX` Source/destination wildcard (Option 3).

`vlan <1-4094>` VLAN identifier.

`inner-vlan <1-4094>`
: Inner VLAN identifier.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#10 permit response ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
(config-arp-acl)#no 10
```

clear access-list

Use this command to clear the access-list counters.

Command Syntax

```
clear access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear access-list counters
```

clear arp access-list

Use this command to clear the ARP access-list counters.

Command Syntax

```
clear arp access-list (NAME|) counters
```

Parameters

NAME	ARP access list name

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear arp access-list counters
```

clear ip access-list

Use this command to clear the IP access-list counters.

Command Syntax

```
clear ip access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip access-list counters
```

clear ipv6 access-list

Use this command to clear the IPv6 access-list counters.

Command Syntax

```
clear ipv6 access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 access-list counters
```

clear mac access-list

Use this command to clear the MAC access-list counters.

Command Syntax

```
clear mac access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mac access-list counters
```

ip access-group

Use this command to attach an IP access list to an interface or terminal line to filter incoming or outgoing IP packets.

Use the `no` form of this command to detach an IP access list from an interface or terminal line.

Note: An egress IP ACL is supported on physical and lag interfaces only. An egress IP ACL will match only routed traffic and not switched traffic. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

Command Syntax

```
ip access-group NAME (in|out)
no ip access-group NAME (in|out)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets
`out`	Filter outgoing packets.

Command Mode

Line mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#hardware-profile filter ingress-ipv4-ext enable

(config)#interface xe3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#no ip access-group mylist in
(config-if)#exit

(config)#line vty
(config-all-line)#ip access-group mylist in
```

Usage: VLANs and LAGs

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Usage: TCAM Groups

An access-group in the egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends to avoid such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

To attach an IP ACL in the ingress direction the `ingress-ipv4` or `ingress-ipv4-ext` TCAM group needs to be enabled and to attach an IP ACL in the egress direction the `egress-ipv4` TCAM group needs to be enabled. See the hardware-profile filter commands for details.

Usage: VTY Interfaces

You can create ACLs for VTY interfaces to filter packets from management applications such as SSH, Telnet, NTP, SNMP, and SNMP traps. TCP, UDP, and ICMP are supported.

For an ACL for VTY, you create the ACL, configure it with rules, and associate the ACL to the terminal line in line mode.

VTY ACLs do not support the following:

- The default rule `deny all`. You must explicitly set up a `deny all` rule based on your requirements.
- VLAN-specific rules.
- Rules with TCP flags.
- Rules with `dscp`, `fragments`, `log`, `precedence`, and `sample` parameters.
- Rules with ICMP code and message types.

ip access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming IP packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the no form of this command to remove an ACL.

Command Syntax

```
ip access-list NAME
no ip access-list NAME
```

Parameters

NAME	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
```

ip access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IP packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#default permit-all
```

ip access-list filter

Use this command to configure access control entry in an access control list (ACL).

This determines whether to accept or drop an IP packet based on the configured match criteria.

Use the no form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring the same filter again with change of sequence number or change of action results in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip|ipcomp|ipv6ip
  |ospf|pim|rsvp|vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D|host A.B.C.D|any) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (precedence (<0-7>| critical| flash | flashoverride| immediate|
  internet| network| priority| routine))|) (vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(<0-255> |ahp | any | eigrp | esp | gre | ipip |
  ipcomp | ipv6ip | ospf | pim | rsvp| vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D | host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63> |af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef )|) (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>)
```

Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
<0-255>	IANA assigned protocol number.
any	Any protocol packet.
ahp	Authentication Header packet.
eigrp	Enhanced Interior Gateway Routing Protocol packet.
esp	Encapsulating Security Payload packet.
gre	Generic Routing Encapsulation packet.
ipip	IPv4 over IPv4 encapsulation packet.
ipcomp	IP Payload Compression Protocol packet.
ipv6ip	IPv6 over IPv4 encapsulation packet.
ospf	Open Shortest Path First packet.
pim	Protocol Independent Multicast packet
rsvp	Resource Reservation Protocol packet.
vrrp	Virtual Router Redundancy Protocol packet.
A.B.C.D/M	Source IP prefix and length.

`A.B.C.D A.B.C.D`	
	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.
`A.B.C.D/M`	Destination IP prefix and length.
`A.B.C.D A.B.C.D`	
	Destination IP address and mask.
`host A.B.C.D`	A single destination host IP address.
`any`	Match any destination IP address.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`precedence`	Match packets with given precedence value.
`<0-7>`	Enter precedence value 0-7.
`critical`	Match packets with critical precedence (5).
`flash`	Match packets with flash precedence (3).
`flashoverride`	Match packets with flash override precedence (4).
`immediate`	Match packets with immediate precedence (2).
`internet`	Match packets with internetwork control precedence (6).

`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`vlan`	Match packets with given vlan value.
`<1 - 4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner vlan value.
`<1 - 4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#11 permit any 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
(config-ip-acl)#no 11
```

ip access-list icmp

Use this command to permit or deny ICMP packets based on the given source and destination IP address. Even DSCP, precedence, vlan ID and inner vlan ID can be configured to permit or deny with the given values.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) ((dscp (<0-63>|af11| af12| af13|
  af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6|
  cs7| default| ef ))| (precedence (<0-7>| critical| flash |
  flashoverride|immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>| critical| flash |
  flashoverride|immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
```

Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
icmp	Internet Control Message Protocol packet.
A.B.C.D/M	Source IP prefix and length.
A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.
A.B.C.D/M	Destination IP prefix and length.
A.B.C.D A.B.C.D	Destination IP address and mask.
host A.B.C.D	A single destination host IP address.
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.

af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.
inner-vlan	Match packets with given inner-vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-icmp
(config-ip-acl)#200 permit icmp any any
```

ip access-list remark

Use this command to add a description to a named IPv4 access control list (ACL).

Use the no form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

LINE	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#remark permit the inside admin address
(config-ip-acl)#exit

(config)#ip access-list mylist
(config-ip-acl)#no remark
(config-ip-acl)#exit
```

ip access-list resequence

Use this command to modify sequence numbers of the IP access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Default

None

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#resequence 5 5
(config-ip-acl)#end
```

ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming TCP or UDP IP packet based on the specified match criteria. This form of command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: TCP flags options and range options like neq, gt, lt and range are not supported by hardware in egress direction.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
  |exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
  uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef)) |(precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine)) |)
  ({ack|established|fin|psh|rst|syn|urg}|) vlan <1-4094>|)(inner-vlan <1-4094>|)

(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix|domain|
  echo|isakmp|mobile-ip |nameserver | netbios-dgm | netbios-ns| netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp
  |time|who|xdmcp) | range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt |lt|neq)(<0-65535> |biff |bootpc |bootps| discard| dnsix|
  domain| echo| isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp |ntp|pim-auto- rp| rip| snmp| snmptrap| sunrpc| syslog| tacacs|
  talk| tftp| time| who| xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11|
  af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|)(inner-vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
  domain| drip| echo|exec|finger|ftp |ftp-data |gopher |hostname| ident| irc|
  klogin| kshell|login|lpd|nntp|pim-auto-rp |pop2 |pop3 |smtp| ssh| sunrpc| tacacs
  |talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any)((eq|gt|lt|neq) (<0-65535> |bgp |chargen |cmd
  |daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data| gopher| hostname|
  ident| irc| klogin| kshell| login| lpd| nntp| pim-auto-rp | pop2| pop3| smtp |ssh
  |sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|)
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>|
  critical| flash | flashoverride| immediate| internet| network| priority|
```

```
    routine)) |) ({ack|established|fin|psh|rst|syn|urg}|)(vlan <1-4094>|)(inner-vlan
    <1-4094>|)
no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
    ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
    domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
    ss|non500-isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|
    tftp|time|who|xdmcp) | range <0-65535> <0-65535>|)(A.B.C.D/M|A.B.C.D A.B.C.D|host
    A.B.C.D| any) ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
    domain|echo| isakmp|mobile- ip|nameserver|netbios-dgm|netbios-ns|netbios-
    ss|non500-isakmp| ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|
    tacacs|talk|tftp|time|who|xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>|
    af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2|
    cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
    flashoverride| immediate| internet| network| priority| routine)) |)(vlan <1-
    4094>|)(inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`A.B.C.D/M`	Source or destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source or destination IP address and mask.
`host A.B.C.D`	Source or destination host IP address.
`any`	Any source or destination IP address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.

`exec`	EXEC.
`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nntp`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34.

af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Precedence.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.
mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.

`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`rip`	Routing Information Protocol.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.
`syslogS`	ystem Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end
```

ipv6 access-group in

Use this command to attach an IPv6 access list to an interface to filter incoming IPv6 packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the no form of this command to detach an IPv6 access list.

Note: To attach IPv6 ACL in the ingress direction ingress-ipv6 TCAM group needs to be enabled. See the hardware-profile filter command for details.

Command Syntax

```
ipv6 access-group NAME in
no ipv6 access-group NAME in
```

Parameters

NAME	Access list name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#permit ipv6 any any
(config-ipv6-acl)#exit
(config)#hardware-profile filter ingress-ipv6 enable

(config)#interface xe3
(config-if)#ipv6 access-group mylist in

(config)#interface xe3
(config-if)#no ipv6 access-group mylist in
```

ipv6 access-list

Use this command to define a IPv6 access control list (ACL) that determines whether to accept or drop an incoming IPv6 packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the no form of this command to remove the ACL.

Command Syntax

```
ipv6 access-list NAME
no ipv6 access-list NAME
```

Parameters

NAME	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#exit
```

ipv6 access-list default

Use this command to modify the default rule action of IPv6 access-list. Default rule is applicable only when IPv6 access-list is attached to interface. Default rule will have the lowest priority and only the IPv6 packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ipv6-acl-01
(config-ipv6-acl)#default permit-all
```

ipv6 access-list filter

Use this command to define an access-control entry in an access control list (ACL) that determines whether to accept or drop an IPv6 packet based on the criteria specified. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address
- DSCP value
- VLAN identifier

Use the no form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: For IPv6 source and destination address filters, only the network part from the address (upper 64 bits) is supported due to hardware restriction. If the address length is more than 64 bits, it cannot be applied on the interfaces but it can be used with distributed lists in control plane protocols.

Command Syntax

```
(<1-268435453>|) (deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22| af23|
  af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef
  )|) (vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22| af23|
  af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef
  )|) (vlan <1-4094>|)
no (<1-268435453>)
```

Parameters

<1-268435453>	IPv6 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
<0-255>	IANA assigned protocol number.
any	Any protocol packet.
ahp	Authentication Header packet.
eigrp	Enhanced Interior Gateway Routing Protocol packet.
esp	Encapsulating Security Payload packet.
gre	Generic Routing Encapsulation packet.
ipipv6	IPv4 over IPv6 Encapsulation packet.
ipcomp	IP Payload Compression Protocol packet.
ipv6ipv6	IPv6 over IPv6 Encapsulation packet.

ospf	Open Shortest Path First packet.
pim	Protocol Independent Multicast packet
rsvp	Resource Reservation Protocol packet.
vrrp	Virtual Router Redundancy Protocol packet.
X:X::X:X/M	Source Address with network mask length.
X:X::X:X X:X::X:X	
	Source Address with wild card mask.
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X X:X::X:X	
	Destination address with wild card mask.
any	Any destination address
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#permit ipipv6 any any
(config-ipv6-acl)#end
```

ipv6 access-list icmpv6

Use this command to permit or deny IPv6 ICMP packets with the given source and destination IPv6 address, DSCP value and VLAN ID.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/ M|X:X::X:X X:X::X:X|any) ((dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef)|) (vlan <1-4094>|)
```

```
no (<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) ((dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (vlan <1-4094>|)
```

Parameters

<1-268435453>	IPv6 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
icmpv6	Internet Control Message Protocol packet.
X:X::X:X/M	Source Address with network mask length.
X:X::X:X X:X::X:X	Source Address with wild card mask.
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X X:X::X:X	Destination address with wild card mask.
any	Any destination address
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.

`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit icmpv6 any any
```

ipv6 access-list remark

Use this command to add a description to an IPv6 access control list (ACL).

Use the no form of this command to remove an access control list description.

Command Syntax

```
remark LINE
no remark
```

Parameters

LINE	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)# remark Permit the inside admin address
```

ipv6 access-list resequence

Use this command to modify sequence numbers of the IPv6 access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting Sequence number.
`INCREMENT`	Sequence number increment steps.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#resequence 15 15
```

ipv6 access-list sctp

Use this command to allow ACL to permit or deny SCTP packets based on the given source and destination IPV6 address. Even DSCP and vlan ID can be configured to permit or deny with the given values.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Range options like neq, gt, lt and range are not supported by hardware in egress direction.

Command Syntax

```
(<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <0-
  65535>)|  } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33|
  af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) (vlan <1-
  4094>|)
no (<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535>
  <0-65535>)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33|
  af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) (vlan <1-
  4094>|)
```

Parameters

<1-268435453>	IPv6 ACL sequence number.
deny	Drop the packet.
permit	Accept the packet.
sctp	Stream Control Transmission Protocol packet.
X:X::X:X/M	Source address with network mask length.
X:X::X:X	Source address with wild card mask.
X:X::X:X	Source address's wild card mask (ignored bits).
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X	Destination address with wild card mask.
X:X::X:X	Destination address's wild card mask (ignored bits).
any	Any destination address.
eq	Source or destination port equal to.
gt	Source or destination port greater than.
lt	Source or destination port less than.
neq	Source or destination port not equal to.
<0-65535>	Source or destination port number.
range	Range of source or destination port numbers:
<0-65535>	Lowest value in the range.
<0-65535>	Highest value in the range.

`dscp`	Match packets with given DSCP value.
`<0-63>`	DSCP value.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit sctp any any
```

ipv6 access-list tcp|udp

Use this command to define a IPv6 access control list (ACL) specification that determines whether to accept or drop an incoming IPv6 packet based on the criteria that you specify. This form of this command filters packets based on source and destination IPv6 address along with protocol (TCP or UDP) and port.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Range options such as neq, gt, lt and range are not supported by the hardware in the egress direction.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any)((eq|gt|lt|neq) <0-65535>|bgp|chargen|cmd|daytime|discard|domain
  |drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk| telnet|time
  |uucp|whois|www) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12| af13|
  af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
  cs6| cs7| default| ef)) (vlan <1-4094>|)

(<1-268435453>|) (deny|permit) udp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain
  |echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk
  |tftp|time|who|xdmcp) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix
  |domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk
  |tftp|time|who|xdmcp) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef) (vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|gt|lt|neq) <0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin
  |kshell|login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0- 65535> <0-65535>)|) (dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef) | (vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) udp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain|echo
  |isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time
  |who|xdmcp) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain|echo
```

```
|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time
|who|xdmcp) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12| af13|
af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
cs6| cs7| default| ef) | (vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`X:X::X:X/M`	Source or destination IPv6 prefix and length.
`X:X::X:X X:X::X:X`	Source or destination IPv6 address and mask.
`any`	Any source or destination IPv6 address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`ftp`	File Transfer Protocol (21).
`ssh`	Secure Shell (22).
`telnet`	Telnet (23).
`www`	World Wide Web (HTTP 80).
`tftp`	Trivial File Transfer Protocol (69).
`bootp`	Bootstrap Protocol (BOOTP) client (67).
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.
`exec`	EXEC.
`finger`	Finger.

`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nnt`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	DSCP value.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.

`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`biff`	Biff.
`bootpc`	Bootstrap Protocol (BOOTP) client.
`bootps`	Bootstrap Protocol (BOOTP) server.
`discard`	Discard.
`dnsix`	DNSIX security protocol auditing.
`domain`	Domain Name Service.
`echo`	Echo.
`isakmp`	Internet Security Association and Key Management Protocol.
`mobile-ip`	Mobile IP registration.
`nameserver`	IEN116 name service.
`netbios-dgm`	Net BIOS datagram service.
`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`rip`	Routing Information Protocol.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.
`syslog`	System Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#deny udp any eq tftp any
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fdf2:860a:746a:e49c::/64 eq ssh
```

mac access-group

Use this command to attach a MAC access list to an interface to filter incoming packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the `no` form of this command to detach a MAC access group.

Note: To attach a MAC ACL in the ingress direction ingress-l2 or ingress-l2-ext TCAM group needs to be enabled and to attach a MAC ACL in the egress direction egress-l2 TCAM group needs to be enabled. See the hardware-profile filter command for details.

Note: An egress ACL is supported on physical and lag interfaces only. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

Command Syntax

```
mac access-group NAME (in|out)
no mac access-group NAME (in|out)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets.
`out`	Filter outgoing packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#permit any any
(config-mac-acl)#exit

(config)#hardware-profile filter ingress-l2-ext enable
```

```
(config)#interface xe3
(config-if)#mac access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#no mac access-group mylist in
(config-if)#exit
```

mac access-list

Use this command to define a MAC access control list (ACL) that determines whether to accept or drop an incoming packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the no form of this command to remove an ACL.

Command Syntax

```
mac access-list NAME
no mac access-list NAME
```

Parameters

NAME	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#exit
```

mac access-list default

Use this command to modify the default rule action of mac access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#default permit-all
```

mac access-list filter

Use this command to define an access control entry (ACE) in a mac access control list (ACL) that determines whether to permit or deny packets with the given source and destination MAC, ether type, cos and VLAN values.

Use the no form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Ether type option is not supported by hardware in egress direction

Command Syntax

```
(<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|)(inner-vlan <1-4094>|)
no (<1-268435453>)
```

Parameters

deny	Drop the packet.
permit	Accept the packet.
<1-268435453>	IPv4 ACL sequence number.
any	Source/Destination any.
XX-XX-XX-XX-XX-XX	Source/Destination MAC address (Option 1).
XX:XX:XX:XX:XX:XX	Source/Destination MAC address (Option 2).
XXXX.XXXX.XXXX	Source/Destination MAC address (Option 3).
XX-XX-XX-XX-XX-XX	Source/Destination wildcard (Option1).
XX:XX:XX:XX:XX:XX	

	Source/Destination wildcard (Option2).
XXXX.XXXX.XXXX	
	Source/Destination wildcard (Option3).
host	A single source/destination host.
aarp	Ethertype - 0x80f3.
appletalk	Ethertype - 0x809b.
decnet-iv	Ethertype - 0x6003.
diagnostic	Ethertype - 0x6005.
etype-6000	Ethertype - 0x6000.
etype-8042	Ethertype - 0x8042.
ip4	Ethertype - 0x0800.
ip6	Ethertype - 0x86dd.
mpls	Ethertype - 0x8847.
lat	Ethertype - 0x6004.
lavc-sca	Ethertype - 0x6007.
mop-console	Ethertype - 0x6002.
mop-dump	Ethertype - 0x6001.
vines-echo	Ethertype - 0x0baf.
WORD	Any Ethertype value.
cos <0-7>	Cos value.
vlan <1-4094>	VLAN identifier.
inner-vlan <1 - 4094>	
	Inner-VLAN identifier.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#permit 0000.1234.1234 0000.0000.0000 any
```

mac access-list remark

Use this command to add a description to a MAC access control list (ACL).

Use the no form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

LINE	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)# remark Permit the inside admin address
```

mac access-list resequence

Use this command to modify sequence numbers of mac access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#resequence 15 15
```

show access-lists

Use this command to display a list of access list

Command Syntax

```
show access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show access-lists expanded
IP access list Iprule1
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
default deny-all
MAC access list Macrule1
10 permit host 0000.1234.1234 any
default deny-all
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
default deny-all

#show access-lists summary
IPV4 ACL Iprule1
statistics enabled
Total ACEs Configured: 1
Configured on interfaces:
xe3/1 - egress (Router ACL)
Active on interfaces:
xe1/3 - ingress (Router ACL)
MAC ACL Macrule1
statistics enabled
Total ACEs Configured: 0
Configured on interfaces:
Active on interfaces:
IPV6 ACL ipv6-acl-01
```

```
statistics enabled
Total ACEs Configured: 2
Configured on interfaces:
xe7/1 - ingress (Router ACL)
Active on interfaces:
```

show arp access-lists

Use this command to display ARP access lists.

Note: Broadcast ARP request packets are counted twice.

Command Syntax

```
show arp access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	ARP access-list name.
expanded	Expanded access-list.
summary	Access-list summary.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show arp access-lists
ARP access list arp1
        10 permit ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
        20 deny ip 2.2.2.0/24 mac any
        default deny-all

#show arp access-lists summary
ARP ACL arp1
       statistics enabled
       Total ACEs Configured: 2
       Configured on interfaces:
          xe1 - ingress (Port ACL)
       Active on interfaces:
          xe1 - ingress (Port ACL)
```

show ip access-lists

Use this command to display IP access lists.

Note: In Qumran devices, when both ip access-list and mac access-list configured on the same interface with rules from both access-lists matching the packet, the match packet statistics is incremented only for the access-list whose hardware-profile filter is configured at the last. Also, when qos is configured on the same interface, along with ingress-acl statistics profile, ingress-qos statistics profile need to be enabled in order to get statistics for both qos entries and acl entries.

Note: See hardware-profile filter for filter groups and hardware-profile statistics.

Command Syntax

```
show ip access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Access-list summary.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip access-lists
IP access list Iprule2
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
default deny-all

#show ip access-lists summary
IPV4 ACL Iprule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa1 - ingress (Port ACL)
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

```
xe3/1 - egress (Router ACL)
Active on interfaces:
sa1 - ingress (Port ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

show ipv6 access-lists

Use this command to display IPv6 access lists.

Command Syntax

```
show ipv6 access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 access-lists
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
20 permit ahp 78fe::1/48 68fe::1/48
30 permit ahp 3333::1/64 4444::1/48 fragments
40 permit ahp 5555::1/64 4444::1/48 dscp af23
default deny-all

#show ipv6 access-lists summary
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

show mac access-lists

Use this command to display MAC access lists.

Note: In Qumran devices, when both ip access-list and mac access-list configured on the same interface with rules from both access-lists matching the packet, match packet statistics is incremented only for the access-list whose hardware-profile filter is configured at the last. Also, when qos is configured on the same interface, along with ingress-acl statistics profile, ingress-qos statistics profile need to be enabled in order to get statistics for both qos entries and acl entries.

Note: See hardware-profile filter for filter groups and hardware-profile statistics.

Command Syntax

```
show mac access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac access-lists
MAC access list Macrule2
default deny-all
MAC access list Macrule3
10 permit host 0000.1234.1234 any
20 deny host 1111.1111.AAAA any 65535
30 permit host 2222.2222.AAAA any 65535
40 permit 0000.3333.3333 0000.0000.FFFF 4444.4444.4444 0000.0000.FFFF
default deny-all [match=1126931077]

# show mac access-lists summary
MAC ACL Macrule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
```

```
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

show running-config access-list

Use this command to show the running system status and configuration details for MAC and IP access lists.

Command Syntax

```
show running-config access-list
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config access-list
ip access-list abd
10 deny any any any
!
mac access-list abc
remark test
10 deny any any
!
```

show running-config aclmgr

Use this command to display the entire access list configurations along with the attachment to interfaces.

Command Syntax

```
show running-config aclmgr (all|)
```

Parameters

`all`	Show running config with defaults

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config aclmgr
ip access-list ip-acl-01
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
mac access-list mac-acl-01
10 permit host 0000.1234.1234 any
20 permit host 0000.1111.AAAA any ipv4 cos 3 vlan 3
!
ipv6 access-list ipv6-acl-01
10 deny ipv6 3ffe::/64 4ffe::/64 dscp af43
20 permit ipv6 78fe::/64 68fe::/64 dscp cs3
!
interface xe1/1
ip access-group ip-acl-01 in
!
```

show running-config ipv6 access-list

Use this command to show the running system status and configuration details for IPv6 access lists.

Command Syntax

```
show running-config ipv6 access-list
```

Parameters

None

Default

None

Command Mode

Privileged exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config ipv6 access-list
ipv6 access-list test
10 permit any any any
```

CHAPTER 6 Access Control List Commands (Standard)

This chapter is a reference for the standard Access Control List (ACL) commands:

ip access-list standard

Use this command to define a standard IP access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IP packet based on the source IP address, either an exact match or a range of prefixes.

Standard ACL can be used by L3 and SNMP protocols to permit or deny IP packets from a host or a range of prefixes.

Use the no form of this command to remove the ACL.

Note: Standard access-lists are not allowed to be attached on interfaces and are used for protocol level filtering purposes.

Command Syntax

```
ip access-list standard NAME
no ip access-list standard NAME
```

Parameters

NAME	Standard IP access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ip access-list standard ip-acl-01
(config-ip-acl-std)#exit
(config)#no ip access-list standard ip-acl-01
```

ip access-list standard filter

Use this command to configure access control entry in an access control list (ACL).

This command determines whether to accept or drop a packet based on the configured source IP address.

Use the no form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
no (deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
```

Parameters

deny	Drop the packet.
permit	Accept the packet.
A.B.C.D/M	Source IP prefix and length.
A.B.C.D A.B.C.D	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.

Default

No default value is specified

Command Mode

Standard IP access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl-std)#permit 30.30.30.0/24
(config-ip-acl-std)#no permit 30.30.30.0/24
```

Ipv6 access-list standard

Use this command to define a standard IPv6 access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IPv6 packet based on the source IPv6 address, either an exact match or a range of prefixes.

Standard IPv6 ACL can be used by L3 protocols to permit or deny IPv6 packets from a host or a range of prefixes.

Use the no form of this command to remove the ACL.

Note: Standard access-lists are not allowed to be attached on interfaces and are used for protocol level filtering purposes.

Command Syntax

```
ipv6 access-list standard NAME
no ipv6 access-list standard NAME
```

Parameters

NAME	Standard IPv6 access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#exit
(config)#no ipv6 access-list standard ipv6-acl-01
```

ipv6 access-list standard filter

Use this command to configure access control entry in an access control list (ACL).This determines whether to accept or drop a packet based on the configured IPv6 prefix.

Use the no form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
no(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
```

Parameters

deny	Drop the packet.
permit	Accept the packet.
X:X::X:X/M	Source address with network mask length.
X:X::X:X X:X::X:X	Source address with wild card mask.
any	Any source address.

Default

No default value is specified

Command Mode

Standard IPv6 access-list mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#permit 2000::0/64
(config-ipv6-acl-std)#no permit 2000::0/64
```

Chassis Monitoring Module Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Chassis Management Module Commands

This chapter provides a description, syntax, and examples of CMM feature commands:

You can retrieve the same set of information through SNMP that these commands display. This MIB is defined in `CMM-CHASSIS-MIB.txt:`

IP Infusion Inc. enterprise identifier	36673
Chassis MIB identifier	100

The MIB definition is available at:

- https://github.com/IPInfusion/OcNOS/branches

Navigate to the directory for the version of OcNOS that you are using.

cpu-core-usage

Use this command to configure user threshold values for monitoring CPU core use.

Use no form of this command to set default thresholds.

Command Syntax

```
cpu-core-usage warning <51-100> alarm <91-100>
```

Parameters

<51-100>	Warning threshold
<91-100>	Alarm threshold

Defaul

Check the default thresholds using `show system-information cpu-load` CLI command.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#cpu-core-usage warning 56 alarm 97
(config)#end
#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 20 Minutes 12 Seconds

Load Average(1 min)       : 4.24% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.87% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.37% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 2.02%
CPU core 1 Usage          : 0.89% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 3 Usage          : 5.41% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 4 Usage          : 2.68% (Crit Thresh : 56%, Alert Thresh : 97%)

#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no cpu-core-usage
(config)#end
#show system-information cpu-load
```

```
System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 21 Minutes 46 Seconds

Load Average(1 min)       : 2.44% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.49% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.27% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 1.82%
CPU core 1 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 4.59% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 1.82% (Crit Thresh : 50%, Alert Thresh : 90%)
#
```

debug cmm

Use this command to enable or disable debugging for CMM.

Command Syntax

```
debug cmm
no debug cmm
```

Parameters

None

Default

By default, debug command is not configured.

Command Mode

Configuration mode and exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug cmm
(config)#no debug cmm
```

locator led

Use this command to turn on the locator LED.

Use the no form of this command to turn off the locator LED.

Command Syntax

```
locator-led on
no locator-led
```

Parameters

None

Default

By default, locator LED is turned off.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#locator-led on
(config)#no locator-led
```

show hardware-information

Use this command to display hardware information.

Command Syntax

```
show hardware-information (memory|fan|temperature|led|power|transceiver|all)
```

Parameter

`all`	Hardware details of all modules.
`fan`	Fan status of the boards.
`led`	LED status of the boards.
`memory`	Memory information of the boards.
`power`	PSU information.
`temperature`	Temperature sensor information of the boards.
`transceiver`	Transceiver presence status and supported list of transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show hardware-information all
-------------------------------------------------------
                RAM INFORMATION
-------------------------------------------------------

Total                                    : 7989 MBytes
Used                                     : 870 MBytes
Free                                     : 7119 MBytes
Shared                                   : 0 MBytes
Buffers                                  : 152 MBytes
Total Swap                               : 0 MBytes
Free Swap                                : 0 MBytes
Current Processes                        : 165
Total High Memory                        : 0 MBytes
Available High Memory                    : 0 MBytes
Unit Size                                : 1 Bytes

-------------------------------------------------------
                HARD DISK INFORMATION
-------------------------------------------------------

Serial Number                            : B06150190009000000FC
```

```
Model Number                                : 16GB SATA Flash Drive
Firmware Revision                           : SFDDA01C16GB SATA Flash Drive
Cylinders                                   : 16383
Heads                                       : 16
Sectors                                     : 31277232
Unformatted Bytes/Track                     : 0
Unformatted Bytes/Sector                    : 0
Revision No                                 : 496.0
Total Size                                  : 14.9 GB

-------------------------------------------------
FAN TRAY             FAN                    RPM
-------------------------------------------------
1                    1                      7021
1                    2                      7021
2                    1                      7021
2                    2                      7021
3                    1                      7072
3                    2                      7021

Board Temp Sensors Temperature
-------------------------------------------------------------------------------
SENSOR TYPE                                  CURRENT TEMP         OPERATING
RANGE
                                             (Degree C)           (Degree C)
-------------------------------------------------------------------------------
Trident2                                     29.0                 <0 - 75>
Nic                                          22.0                 <0 - 70>
Ambient                                      23.0                 <0 - 75>

BCM Chip Internal Temperature
-----------------------------------------------------
TEMP MONITOR         CURRENT TEMP         PEAK TEMP
                     (Degree C)           (Degree C)
-----------------------------------------------------
0                    41.1                 42.2
1                    42.2                 43.3
2                    40.6                 41.7
3                    40.6                 41.7
4                    40.0                 41.1
5                    40.6                 41.1
6                    39.5                 40.6
7                    39.5                 40.6
Average Current Temperature: 40.5C

-----------------------------------------------------
                System Power Information
-----------------------------------------------------
VCC 5V POWER RAIL                       : GOOD
VCC 3.3V POWER RAIL                     : GOOD
VCC 1.05V POWER RAIL                    : GOOD
VCC 1.5V POWER RAIL                     : FAIL
VCC 1.8V POWER RAIL                     : FAIL
MAC 1V POWER RAIL                       : GOOD
MAC AVS 1V POWER RAIL                   : GOOD
POWER VDDR                              : GOOD
3.3V POWER RAIL                         : FAIL
```

```
    1.8V POWER RAIL                          : FAIL
    1.05V POWER RAIL                         : GOOD
    1.5V POWER RAIL                          : GOOD
    VCC POWER RAIL                           : GOOD
    1.5V SB POWER RAIL                       : FAIL
    MAIN BOARD POWER RAIL                    : GOOD
    HOT SWAP1 POWER RAIL                     : GOOD
    HOT SWAP2 POWER RAIL                     : GOOD
    CMM_PS1_12V_PG                           : FAIL
    CMM_PS2_12V_PG                           : GOOD
```

PSU	VOLT-IN (Volt)	VOLT-OUT (Volt)	CURR-IN (Ampere)	CURR-OUT (Ampere)	PWR-IN (Watt)	PWR-OUT (Watt)	TEMP-1 (Celsius)	TEMP-2 (Celsius)	FAN-1 (Rpm)	FAN-2 (Rpm)
Max						460.00				
2	118.25	11.92	0.83	7.25	97.75	86.38	30.50	29.00	2040.00	NA

```
    ------------------------------------------------
    LED              STATE               DESCRIPTION
    ------------------------------------------------
    POWER            BLINKING YELLOW     Power Supply Failed
    FAN TRAY 1       GREEN               Normal
    FAN TRAY 2       GREEN               Normal
    FAN TRAY 3       GREEN               Normal
    SYSTEM           GREEN               Normal
    MASTER           GREEN               Unit in Master mode
    LOCATOR          OFF
    FRONT FAN        GREEN               Fan is Normal

    ------------------------------------------------------
              Transceiver DDM support list
    ------------------------------------------------------
    Type                         :QSFP
    Vendor Name                  :AVAGO
    Vendor Part Number           :AFBR-79E4Z
    DDM Supported                :Yes


    ----------------------------------------
    PORT NO    TYPE       STATUS
    ----------------------------------------
    1          QSFP       Not Present
    2          QSFP       Present
    3          QSFP       Not Present
    4          QSFP       Present
    5          QSFP       Not Present
    6          QSFP       Present
    7          QSFP       Not Present
    8          QSFP       Present
    9          QSFP       Present
    10         QSFP       Not Present
    11         QSFP       Present
    12         QSFP       Not Present
    13         QSFP       Not Present
    14         QSFP       Not Present
    15         QSFP       Not Present
    16         QSFP       Not Present
    17         QSFP       Not Present
```

```
18          QSFP        Not Present
19          QSFP        Not Present
20          QSFP        Not Present
21          QSFP        Present
22          QSFP        Present
23          QSFP        Not Present
24          QSFP        Not Present
25          QSFP        Not Present
26          QSFP        Not Present
27          QSFP        Not Present
28          QSFP        Present
29          QSFP        Not Present
30          QSFP        Present
31          QSFP        Not Present
32          QSFP        Present
```

Table 1-75 explains the show command output fields.

Table 1-75: show hardware-information all output

Entry	Description
Ram Information	Displays the used memory, free memory, shared, buffers, total swap, and free swap memory.
Hard Disk Information	Displays hard drive serial number, model, firmware revision, cylinders, heads, and sectors, as well as revision number and total size.
Fans	Displays the fan tray numbers, numbers of fans per tray, and their speed in RPM.
Board Temp Sensors Temperature	Displays sensor type, current temperature, and operating range.
BCM Chip Internal Temperature	Displays broadcom chips current internal temperature, Operating range and average temperature.
System Power Information	Displays system power Information. Shows Voltage on all rails, and whether the power is up or has failed.
PSU	Show main power supply statistics – Volts in, Volts out, current in and out Amperes, power in and out in Watts, temperature of each power supply, and fan speed in RPM.
LED	Shows a list of what the LEDs represent, what state the LEDs mean, and a description of what the LEDs current color means.
Transceiver DDM support list	Show a list of transceivers that support Digital Diagnostic Monitoring (DDM) – type, vendor name, part number, and whether DDM is supported.
Port Number	Displays a list of the port numbers, port type (SFP,QSFP, etc) and whether a transceiver is or is not in the port.

show system fru

Use this command to display the system FRU controlled by BMC.

Command Syntax

```
show system fru
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show system fru
--------------System FRUs------------------
FRU Device Description : MAINBOARD_FRU
Board Mfg Date        : 2018-09-17 13:34:00
Board Mfg             : UFISPACE
Board Product         : S9500-30XS-Board
Board Serial          : WB2N9470004
Product Manufacturer  : UFISPACE
Product Name          : S9500-30XS
Product Version       : PVT
Product Serial        : WE61A47S00016
Product Asset Tag     : 00

FRU Device Description : PSU0_FRU
Product Manufacturer  : FSPGROUP
Product Name          : VICTO451AM
Product Part Number   : YNEB0450
Product Version       : BM-2R01P10
Product Serial        : T0A060Y322009000053
Product extra 1       : P3H800A03
Product extra 2       : A

FRU Device Description : PSU1_FRU
Product Manufacturer  : FSPGROUP
Product Name          : VICTO451AM
Product Part Number   : YNEB0450
Product Version       : BM-2R01P10
Product Serial        : T0A060Y322009000052
Product extra 1       : P3H800A03
Product extra 2       : A
#
```

show system-information

Use this command to display system information.

Command Syntax

```
show system-information (all|fan|psu|os|cpu|bios|cpu-load|board-info)
```

Parameter

`all`	System information of all modules.
`bios`	BIOS information.
`board-info`	Board EEPROM details.
`cpu`	Processor information.
`cpu-load`	CPU load information.
`fan`	Fan Field Replaceable Units (FRU) EEPROM information.
`os`	OS and Kernel version information.
`psu`	Power Supply Field Replaceable Units (FRU) EEPROM information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system-information psu
System PSU FRU Information
=========================
PSU 2 Country of Origin          : CN
PSU 2 PPID Part Number           : 0T9FNW
PSU 2 PPID Part Number Rev       : A00
PSU 2 Manufacturer ID            : 28298
PSU 2 Date Code                  : 52R
PSU 2 Serial Number              : 0298
PSU 2 Part Number                : 0T9FNW
PSU 2 Part Number Revision       : A00
PSU 2 Number of Fans in the tray : 1
PSU 2 Type                       : AC Normal
PSU 2 Service Tag                : AEIOU
```

The following tables explain the show command output fields.

Table 1-76: show system-information topics

Topic	Description
all	Show all topics of system information..
bios	Display BIOS information.
board-info	Display information related to the board.
cpu	Displays Central Processing Unit information
cpu-load	Displays the load on the system’s CPU.
fan	Displays fan information contain in the EEPROM.
os	Displays information regarding the host operating system
psu	Displays information regarding Field Replaceable Units (FRU).

Table 1-77: Show fan topic displays

System Fan FRU Information	Description
Fan Tray “#” PPID Part Number	The vendor’s part number for the fan.
Fan Tray Serial Number	As stated
Service Tag	The Service Tag can help identify your device for on-line support and upgrading drivers
Vendor Name	As stated

Table 1-78: Show system BIOS information

BIOS Information	Description
# dmidecode	The dmidecode is a tool for dumping a computer's DMI table contents in a human-readable format. This table contains a description of the system's hardware components, as well as other useful pieces of information such as serial numbers and BIOS revisions.
SMBIOS	The System Management BIOS (SMBIOS) defines data structures (and access methods) that can be used to read management information produced by the BIOS of a computer. Also, it is involved with the DMI Address –
Handle 0x0000, DMI type 0, 24 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 0 indicates the following information is specific to BIOS properties, and is 24 bytes long.
BIOS Physical Information	• Vendor – The manufacture of the BIOS. • Version – The Version number. • Release Date – as stated. • Address – starting address (in memory) of the BIOS.

Table 1-78: Show system BIOS information (Continued)

BIOS Information	Description
Characteristics	• Is PCI supported. • Is BIOS upgradeable. • Is boot from a CD supported. • Is selectable boot devices supported. • Is BIOS ROM socketed. • Is Enhanced Disk Drive (EDD) vectoring supported. • Is 5.25"/1.2 MB floppy services supported (int 13h) • Is 3.5"/720 kB floppy services supported (int 13h) • Is 3.5"/2.88 MB floppy services supported (int 13h) • Is Print screen service supported (int 5h) • Is 8042 keyboard services supported (int 9h) • Is Serial services supported (int 14h) • Is Printer services supported (int 17h) • Is Advanced Configuration and Power Interface (ACPI) supported • Is USB legacy supported • Is BIOS boot specification supported • Is Targeted content distribution supported • Is Unified Extensible Firmware Interface (UEFI) supported
BIOS Revision	The BIOS revision number.
Handle 0x0043, DMI type 13, 22 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 13 indicates the following information is specific to BIOS language information, and is 22 bytes long.
BIOS Language Informantion	• Language Description Format – A term that describes the number of bits used to represent the BIOS Language information parameters. • Installable Languages – The number of languages that can be used by the BIOS at any time. • Currently Installed Language – United States English (or Latin-1) as described by the ISO standard, en|US|iso8859-1.

Table 1-79: Show CPU information

System CPU Information	Description
processor	The processor number of each CPU
model name	Details about each CPU. For example, Intel(R) Atom(TM) CPU C2538 @ 2.40GHz.

Table 1-80: Show system CPU load information

Load Information	Description
Uptime	As stated in days, hours, minutes, and seconds.
Load Average for past 1min	As stated in percent.
Load Average for past 5 min	As stated in percent.

Table 1-80: (Continued)Show system CPU load information

Load Information	Description
Load Average for past 15 min	As stated in percent.
CPU Usage at this instant	As stated in percent.
Max threshold for CPU-usage	As stated in percent.

Table 1-81: Show system board information

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated
Manufacture Date	As state
Platform Name	The platform on which the product is based.
ONIE Version	The version of the Open Network Install Environment (ONIE).
MAC addresses	Number of MAC addresses related to the device.
Manufacture	As stated
Country Code	The code that represents the country of manufacture. For example, US = United States, TW = Taiwan, and so on.
Diag Version	As stated
CRC-32	Cyclic Redundancy Check value.
Switch Chip Revision	As stated
MAIN BOARD REVISION	As stated
CPU CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the CPU.
SW CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the switch.
MAIN BOARD TYPE	An identifying string for the main board.
CPU BOARD ID	An identifying string for the CPU board.
CPU BOARD VERSION	As stated
SW BOARD ID	NA
SW BOARD VERSION	As stated
VCC 5V	The state of the VCC 5V power rail (Enabled \ Disabled)
MAC 1V	The state of the MAC 1V power rail Enabled \ Disabled

Table 1-81: (Continued)Show system board information

System Information	Description
VCC 1.8V	The state of the VCC 1.8V power rail (Enabled \ Disabled)
MAC AVS 1V	The state of the MAC AVS 1V power rail (Enabled \ Disabled)
HOT SWAP1	Enabled \ Disabled
HOT SWAP2	Enabled \ Disabled

Table 1-82: Show host system details

Host Information	Description
OS Distribution	The operating system on which the device is to run.
Kernel Version	A string that identifies the operating kernel.

show system sensor

Use this command to display system sensors controlled by BMC.

Command Syntax

```
show system sensor
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show system sensor
-------------------------------------------------System Sensors-------------------------
-------------------------------
Codes: LNR - Lower Non-Recoverable
LCR - Lower Critical
LNC - Lower Non-Critical
UNC - Upper Non-Critical
UCR - Upper Critical
UNR - Upper Non-Recoverable
Note: For discrete sensor, thresholds and value columns are not applicable.

SENSOR          | VALUE      | UNITS      | LNR       | LCR       | LNC       | UNC
| UCR       | UNR       | STATE
-------------------------------------------------------------------------------------
-----------------------------------
Temp_MAC        | 43.000     | degrees C  | na        | na        | na        | 96.000
| 101.000   | 106.000   | ok
Temp_CPU        | 40.000     | degrees C  | na        | na        | na        | 92.000
| 97.000    | 102.000   | ok
Temp_BMC        | 32.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_10GPHY     | 35.000     | degrees C  | na        | na        | na        | 92.000
| 95.000    | 98.000    | ok
Temp_DDR4       | 33.000     | degrees C  | na        | na        | na        | 85.000
| 90.000    | 92.000    | ok
Temp_FANCARD1   | 29.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_FANCARD2   | 27.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
PSU0_Temp       | 37.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
PSU1_Temp       | 28.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
```

```
VSENSE_BMC_P12V  | 12.050     | Volts      | 11.200    | 11.400    | na        | na
| 12.600    | 12.750    | ok
VSENSE_HEATER    | 0.000      | Volts      | na        | na        | na        | 9.900
| 10.000    | 10.100    | ok
VSENSE_BMC_P2V5  | 2.500      | Volts      | 2.320     | 2.360     | na        | na
| 2.640     | 2.680     | ok
VSENSE_1VDDR     | 1.020      | Volts      | 0.900     | 0.940     | na        | na
| 1.060     | 1.080     | ok
VSENSE_BMC_P5VT  | 5.040      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_P5V_SB    | 4.980      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_BMC_1.26V | 1.250      | Volts      | 1.150     | 1.200     | na        | na
| 1.320     | 1.360     | ok
VSENSE_BMC_1.53V | 1.540      | Volts      | 1.380     | 1.460     | na        | na
| 1.610     | 1.690     | ok
VSENSE_BMC_P3V3  | 3.280      | Volts      | 3.020     | 3.140     | na        | na
| 3.480     | 3.640     | ok
FAN_0            | 12900.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_1            | 13000.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_2            | 12400.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_3            | 12300.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_4            | 11800.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
PSU0_FAN         | 8280.000   | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | ok
PSU1_FAN         | 0.000      | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | Lower Non-Recoverable
HWM_VCORE_IN     | 1.000      | Volts      | 0.910     | 0.940     | na        | na
| 1.060     | 1.090     | ok
HWM_P1V0_VIN     | 1.000      | Volts      | 0.900     | 0.950     | na        | na
| 1.050     | 1.070     | ok
HWM_P1V2_VIN     | 1.210      | Volts      | 1.110     | 1.140     | na        | na
| 1.260     | 1.290     | ok
HWM_P1V25_VIN    | 1.250      | Volts      | 1.150     | 1.190     | na        | na
| 1.310     | 1.340     | ok
HWM_P1V8_VIN     | 1.780      | Volts      | 1.660     | 1.710     | na        | na
| 1.900     | 1.950     | ok
HWM_P3V3_VIN     | 3.300      | Volts      | 3.040     | 3.120     | na        | na
| 3.480     | 3.580     | ok
HWM_Temp_MAC     | 35.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_Heater  | 39.000     | degrees C  | -45.000   | -42.000   | -40.000   | 73.000
| 75.000    | 78.000    | ok
HWM_Temp_BMC     | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 80.000
| 85.000    | 89.000    | ok
HWM_Temp_CPU     | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_AMB     | 28.000     | degrees C  | -45.000   | -42.000   | -40.000   | 76.000
| 80.000    | 84.000    | ok
HWM_Temp_PHY3    | 35.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
```

```
CPU_PROC_HOT     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPU_CAT_ERROR    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
CPU_THERMAL_TRIP | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPU_TO_BMC_INT   | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
Thermal_NMI      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_BMC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_PHY_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_MAC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_DDR_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPLD_NMI         | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
VCORE_Fault      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
FAN_CARD_INT     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
BMC_LOADDEFAULT  | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
CPU_BOOT_Done    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
CPU_Presence     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan2_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan3_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan4_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
CPU_POWEROK      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
MB_POWEROK       | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
PSU0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
PSU1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
PSU0_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
PSU1_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Disabled
PSU0_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
PSU1_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
```

```
PSU0_VIN         | 99.000     | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU0_VOUT        | 11.900     | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU0_IIN         | 0.420      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU0_IOUT        | 0.850      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU1_VIN         | 0.000      | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU1_VOUT        | 0.000      | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU1_IIN         | 0.000      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU1_IOUT        | 1.950      | Amps       | na        | na        | na        |  na
| na         | na         | ok
#
```

system-load-average

Use this command to configure user threshold values for monitoring system load average for last 1 minute, 5 minute and 15 minute.

Use no form of this command to set default thresholds.

Command Syntax

```
system-load-average (1min warning <41-100> alarm <51-100> 5min alarm <51-100> 15min
  alarm <51-100>)
```

Parameters

`1min`	1min
`warning`	Warning
`<41-100>`	41-100
`alarm`	alarm
`<51-100>`	51-100
`5min`	5min
`alarm`	alarm
`<51-100>`	51-100
`15min`	15min
`alarm`	alarm
`<51-100>`	51-100

Default

Check the default thresholds using `show system-information cpu-load` CLI command.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#system-load-average 1min warning 45 alarm 55 5min alarm 65 15min
alarm 75

#show system-information cpu-load

System CPU-Load Information
===========================
```

```
Uptime                    : 64 Days 17 Hours 56 Minutes 22 Seconds

Load Average(1 min)       : 5.74% (Crit Thresh : 45%, Alert Thresh : 55%)
Load Average(5 min)       : 3.71% (Crit Thresh : N/A, Alert Thresh : 65%)
Load Average(15 min)      : 3.21% (Crit Thresh : N/A, Alert Thresh : 75%)

Avg CPU Usage             : 4.67%
CPU core 1 Usage          : 4.42% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 2.68% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 6.19% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 5.36% (Crit Thresh : 50%, Alert Thresh : 90%)

#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no system-load-average
(config)#end
#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 16 Minutes 34 Seconds

Load Average(1 min)       : 0.63% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 1.90% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.11% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 2.07%
CPU core 1 Usage          : 1.83% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 6.36% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 0.93% (Crit Thresh : 50%, Alert Thresh : 90%)
```

CHAPTER 2 Digital Diagnostic Monitoring Commands

This chapter provides a description, syntax, and examples of DDM feature commands:

clear ddm transceiver alarm

Use this command to clear the transceiver alarm in the DDM monitor interface.

Command Syntax

```
clear ddm transceiver alarm.
```

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
OCNOS(config-if)#ddm monitor
OCNOS(config-if)#clear ddm transceiver alarm
OCNOS(config-if)#exit
```

clear ddm transceiver alarm all

Use this command to clear the transceiver DDM alarm for all interface.

Command Syntax

clear ddm transceiver alarm all

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OCNOS# clear ddm transceiver alarm all
```

ddm monitor

Use this command to enable or disable DDM monitoring for interfaces which have a supported transceiver.

Use the no form of this command to remove DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor (disable|enable)
no ddm monitor
```

Parameters

`enable`	Enable DDM monitoring.
`disable`	Disable DDM monitoring.

Default

By default, DDM monitoring is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ddm monitor enable
(config-if)#ddm monitor disable
(config-if)#exit

(config)#interface xe1
(config-if)#no ddm monitor
(config-if)#exit
```

ddm monitor all

Use this command to enable DDM monitoring for all transceiver.s

Use the no form of this command to disable DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor all
no ddm monitor all
```

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor all

(config)#no ddm monitor all
```

ddm monitor interval

Use this command to set the monitoring interval for the transceiver.

Use no form with this command to set the monitoring interval to its default.

Command Syntax

```
ddm monitor interval <60-3600>
no ddm monitor interval
```

Parameters

<60-3600>	Interval period in seconds.

Default

The default monitoring interval is 60 seconds.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor interval 60
```

debug ddm

Use this command to enable or disable debugging for DDM.

Command Syntax

```
debug ddm
no debug ddm
```

Parameters

None

Default

By default, debug command is not configured.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ddm
(config)#no debug ddm
```

service unsupported-transceiver

Use this command to allow an unsupported transceiver to be enabled for DDM monitoring.

Use the no form of this command to disable DDM on an unsupported transceiver.

Command Syntax

```
service unsupported-transceiver
no service unsupported-transceiver
```

Parameters

None

Default

By default, DDM on an unsupported transceiver is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service unsupported-transceiver

(config)#no service unsupported-transceiver
```

show controller details

Use this command to display the EEPROM details of transceiver.s

Command Syntax

```
show interface (IFNAME|) controllers
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe52/1 controllers

Port Number             : 52
Vendor oui              : 0x0 0x17 0x6a
Vendor name             : AVAGO
Vendor part_no          : AFBR-79E4Z
serial_number           : QB380161
transceiver_type        : QSFP OR LATER
connector_type          : MPO 1x12
qsfp_transceiver_code   : 1X-LX
vendor_rev              : 01
date_code               : 110920   (yymmddvv, v=vendor specific)
encoding                : SONET
br_nominal              : 103     (100 MHz)
length_km               : 0
length_mtr              : 50
length_50mt             : 0
length_62_5mt           : 0
length_cu               : 0
cc_base                 : 0x7d
cc_ext                  : 0x28
DDM Support             : yes
```

show supported-transceiver

Use this command to display supported transceivers.

Command Syntax

```
show supported-transceiver
```

Parameters

None

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#show supported-transceiver
-----------------------------------------------------
          Transceiver DDM support list
-----------------------------------------------------
Type                      :SFP
Vendor Name               :FINISAR CORP
Vendor Part Number        :FTLF8519P2BNL
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :EVERTZ
Vendor Part Number        :SFP10G-TR13S
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :AVAGO
Vendor Part Number        :AFBR-79E4Z
DDM Supported             :Yes
```

show interface transceiver details

Use this command to display details of transceivers and threshold violations.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|)
```

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.
`detail`	Transceiver information such as voltage, temperature, power, and current.
`threshold violation`	Transceiver threshold violations.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface transceiver detail
PORT     Temp     High Alarm High Warn Low Warn Low Alarm
       (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)

-------------------------------------------------------
5        30.060      95          90       -20      -25
6        30.463      95          90       -20      -25
52       34.486      75          70         0       -5
53       30.764      75          70         0       -5

         Voltage  High Alarm High Warn Low Warn Low Alarm
         (Volts)    (Volts)   (Volts)   (Volts)   (Volts)
-------------------------------------------------------
5        3.339       3.900     3.700    2.900     2.700
6        3.365       3.900     3.700    2.900     2.700
52       3.360       3.630     3.465    3.135     2.970
53       3.353       3.630     3.465    3.135     2.970

         Current  High Alarm High Warn Low Warn Low Alarm
          (mA)      (mA)        (mA)      (mA)    (mA)
-------------------------------------------------------
5        6.468       17.000    14.000   2.000     0.034
6        7.014       17.000    14.000   2.000     0.034
52       7.250       10.000    9.500    1.000     0.500
53       7.284       10.000    9.500    1.000     0.500
```

```
          RxPower  High Alarm High Warn Low Warn Low Alarm
          (dBm)      (dBm)      (dBm)     (dBm)    (dBm)
-----------------------------------------------------------
5         0.332       1.259     0.794    0.016     0.010
6         0.321       1.259     0.794    0.016     0.010
52        0.727       2.188     1.738    0.112     0.000
53        0.352       2.188     1.738    0.112     0.000

          TxPower  High Alarm High Warn Low Warn Low Alarm
           (mW)       (mW)       (mW)      (mW)     (mW)
-----------------------------------------------------------
5         0.342       0.631     0.631    0.079     0.067
6         0.342       0.631     0.631    0.079     0.067
```

Table 2-83 explains the output fields.

Table 2-83: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliamperes used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.

Control Plane Policing Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Control Plane Policing Commands

This chapter is a reference for the Control Plane Policing (CoPP) commands.

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax

```
clear interface cpu counters
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface cpu counters
```

cpu-queue

Use this command to set protocol queues shaper and enable/disable queue monitoring for drop.

Command Syntax

```
cpu-queue (cpu.q0|cpu.q1|cpu.q2|cpu.q3|cpu.q4|cpu.q5|cpu.q6|cpu.q7|
  arp|bfd|bgp|bpdu|dsp|icmp-mpls|icmp-redirect|igmp|isis|link-
  local|nhop|ospf|pim|reserved-mc|rsvp-ldp|sflow|vrrp-rip-dhcp|vxlan)(monitor|no-
  monitor|rate <0-100000>)
no cpu-queue (cpu.q0|cpu.q1|cpu.q2|cpu.q3|cpu.q4|cpu.q5|cpu.q6|cpu.q7|
  arp|bfd|bgp|bpdu|dsp|icmp-mpls|icmp-redirect|igmp|isis|link-
  local|nhop|ospf|pim|reserved-mc|rsvp-ldp|sflow|vrrp-rip-dhcp|vxlan)(monitor|no-
  monitor|rate <0-100000>)
```

Parameters

`arp`	ARP queue parameters
`bfd`	BFD queue parameters
`bgp`	BGP queue parameters
`bpdu`	BPDU queue parameters
`cpu.q0`	cpu.q0
`cpu.q1`	cpu.q1
`cpu.q2`	cpu.q2
`cpu.q3`	cpu.q3
`cpu.q4`	cpu.q4
`cpu.q5`	cpu.q5
`cpu.q6`	cpu.q6
`cpu.q7`	cpu.q7
`dsp`	SP queue parameters
`icmp-mpls`	ICMP/MPLS queue parameters
`icmp-redirect`	ICMP-redirect queue parameters
`igmp`	GMP queue parameters
`isis`	ISIS queue parameters
`link-local`	Link-local queue parameters
`nhop`	Next hop queue parameters
`ospf`	OSPF queue parameters
`pim`	PIM queue parameters
`reserved-mc`	Reserved-mc queue parameters
`rsvp-ldp`	RSVP/LDP queue parameters
`sflow`	Sflow queue parameters
`vrrp-rip-dhcp`	VRRP/RIP/DHCP queue parameters
`vxlan`	VXLAN queue parameters

`monitor`	Monitor CPU queue usage
`no-monitor`	Do not monitor CPU queue usage
`rate`	Set CPU queue rate <0-100000>

Default

CPU queues are set with the default values as shown in Table 1-28 and Table 1-29.

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 2.4.

Example

Use the following command to configure rate/monitor/no-monitor for protocol queues:

```
#configure terminal
(config)#cpu-queue cpu-q0 rate 400
```

Use the following command to verify the rate received on each protocol queue:

```
#show int cpu counters rate kbps

Load interval: 30 second
+-------------------+--------------+-------------+--------------+-------------+
|    CPU Queue(%)   |    Rx kbps   |    Rx pps   |    Tx kbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 CPU0.q0      (100%) -              -             470.63         58
 bpdu         (  0%) -              -             0.54           1
```

Use the following command to verify the maximum, configured, and default configuration values:

```
#show cpu-queue details

* - Can not configure the parameter
Cpu queue                  Rate In Kbps                    Monitor Status
Name          Configured  Default   Max Rate Allowed  Configured    Default
============  ==========  =======   ================  ============  ==========
cpu.q0         400           900           900            -       * no-monitor
cpu.q1          -            900           900            -       * no-monitor
cpu.q2          -            900           900            -       * no-monitor
cpu.q3          -            900           900            -       * no-monitor
cpu.q4          -            900           900            -       * no-monitor
cpu.q5          -            900           900            -       * no-monitor
cpu.q6          -            900           900            -       * no-monitor
cpu.q7          -            900           900            -       * no-monitor
igmp            -            1000          1000           -       * no-monitor
is-is           -            8000          8000           -         no-monitor
reserved mc     -            8000          8000           -         no-monitor
link-local      -            1000          1000           -         no-monitor
```

```
ospf            -            8000          8000           -          no-monitor
bgp             -            8000          8000           -          no-monitor
rsvp/ldp        -            1500          1500           -          no-monitor
vrrp/rip/dhcp   -            2000          2000           -          no-monitor
pim             -            8000          8000           -        * no-monitor
icmp            -            1000          1000           -          no-monitor
arp             -            1000          1000           -          no-monitor
bpdu            -            1000          1000           -          no-monitor
bfd             -            1000          1000           -          no-monitor
sflow           -            16384         16384          -          no-monitor
dsp             -            1500          1500           -          no-monitor
vxlan           -            500           500            -          no-monitor
nhop            -            500           500            -          no-monitor
icmp-redirect   -            400           400            -          no-monitor
guest-vm        -            8000          8000           -        * no-monitor
```

Use the following command to remove the configuration:

```
(config)#no cpu-queue cpu.q0
(config)#exit
#
#show cpu-queue details
* - Can not configure the parameter
Cpu queue                  Rate In Kbps                    Monitor Status
Name          Configured  Default   Max Rate Allowed  Configured    Default
===========   ==========  =======   ================  ==========   ==========
cpu.q0          -           900           900           -        * no-monitor
cpu.q1          -           900           900           -        * no-monitor
cpu.q2          -           900           900           -        * no-monitor
cpu.q3          -           900           900           -        * no-monitor
cpu.q4          -           900           900           -        * no-monitor
cpu.q5          -           900           900           -        * no-monitor
cpu.q6          -           900           900           -        * no-monitor
cpu.q7          -           900           900           -        * no-monitor
igmp            -           1000          1000          -        * no-monitor
is-is           -           8000          8000          -          no-monitor
reserved mc     -           8000          8000          -          no-monitor
link-local      -           1000          1000          -          no-monitor
ospf            -           8000          8000          -          no-monitor
bgp             -           8000          8000          -          no-monitor
rsvp/ldp        -           1500          1500          -          no-monitor
vrrp/rip/dhcp   -           2000          2000          -          no-monitor
pim             -           8000          8000          -        * no-monitor
icmp            -           1000          1000          -          no-monitor
arp             -           1000          1000          -          no-monitor
bpdu            -           1000          1000          -          no-monitor
bfd             -           1000          1000          -          no-monitor
sflow           -           16384         16384         -          no-monitor
dsp             -           1500          1500          -          no-monitor
vxlan           -           500           500           -          no-monitor
```

```
nhop            -           500          500           -         no-monitor
icmp-redirect   -           400          400           -         no-monitor
guest-vm        -           8000         8000          -       * no-monitor
```

show interface cpu counters queue-stats

Use this command to display the counters of packets destined to the CPU.

For details about this command, see show interface counters queue-stats.

Example

```
#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |   Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
igmp              (E) 2097152  151               16258               0                 0
reserved mc       (E) 2097152  62826             6324464             0                 0
ospf              (E) 1048576  3184              308548              0                 0
bgp               (E) 1048576  27587             3938124             0                 0
rsvp/ldp          (E) 1048576  29138             3090385             0                 0
icmp              (E) 1048576  176               20924               0                 0
arp               (E) 1048576  751               48064               0                 0
bpdu              (E) 1048576  26833             3129794             0                 0
bfd               (E) 1048576  38                4028                0                 0
dsp               (E) 78643200 507               34476               0                 0
```

show cpu-queue details

Use this command to display CPU queue details.

Command Syntax

```
show cpu-queue details
```

Parameters

None

Default

Not applicable

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 2.4.

Example

Use the following command to configure rate/monitor/no-monitor for protocol queues:

```
#configure terminal
(config)#cpu-queue cpu-q0 rate 400
```

Use the following command to verify the maximum, configured, and default configuration values:

```
#show cpu-queue details

* - Can not configure the parameter
Cpu queue                  Rate In Kbps                    Monitor Status
Name          Configured  Default   Max Rate Allowed  Configured    Default
===========   ==========  =======   ================  ==========   ==========
cpu.q0         400           900           900            -       * no-monitor
cpu.q1          -            900           900            -       * no-monitor
cpu.q2          -            900           900            -       * no-monitor
cpu.q3          -            900           900            -       * no-monitor
cpu.q4          -            900           900            -       * no-monitor
cpu.q5          -            900           900            -       * no-monitor
cpu.q6          -            900           900            -       * no-monitor
cpu.q7          -            900           900            -       * no-monitor
igmp            -            1000          1000           -       * no-monitor
is-is           -            8000          8000           -         no-monitor
reserved mc     -            8000          8000           -         no-monitor
link-local      -            1000          1000           -         no-monitor
ospf            -            8000          8000           -         no-monitor
bgp             -            8000          8000           -         no-monitor
rsvp/ldp        -            1500          1500           -         no-monitor
```

```
vrrp/rip/dhcp   -           2000          2000          -          no-monitor
pim             -           8000          8000          -        * no-monitor
icmp            -           1000          1000          -          no-monitor
arp             -           1000          1000          -          no-monitor
bpdu            -           1000          1000          -          no-monitor
bfd             -           1000          1000          -          no-monitor
sflow           -           16384         16384         -          no-monitor
dsp             -           1500          1500          -          no-monitor
vxlan           -           500           500           -          no-monitor
nhop            -           500           500           -          no-monitor
icmp-redirect   -           400           400           -          no-monitor
guest-vm        -           8000          8000          -        * no-monitor
```

SECTION 5 # Layer 2

Layer 2 Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Spanning Tree Protocol Configuration

This chapter contains a complete sample Spanning Tree Protocol (STP) configuration.

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops. Spanning tree also allows a network design to include redundant links to provide automatic backup paths if an active link fails, thus, eliminating the need to manually enable or disable the backup links.

Topology

The following example is a simple multi-bridge topology.

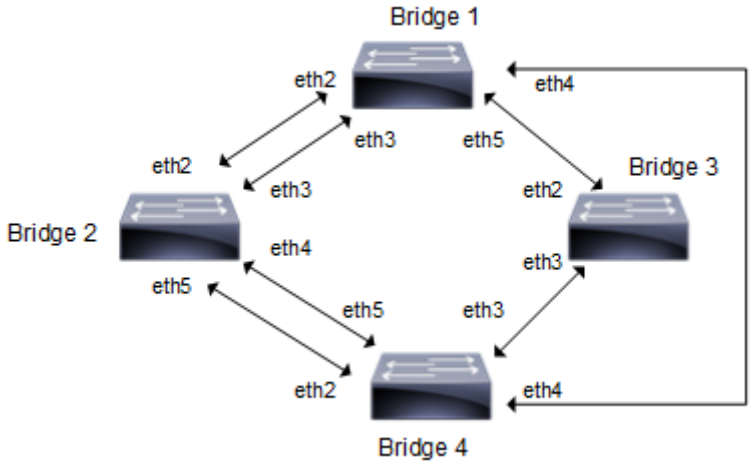


Figure 1-36: STP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configurations

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee`	Add a bridge `(1)` to the spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.

`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee`	Add a bridge (2) to the spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol ieee`	Add a bridge (4) to the spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.

Bridge4(config-if)#switchport	Configure interface as a layer 2 port.
Bridge4(config-if)#bridge-group 4	Associate the interface with bridge group 4.
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth5	Enter interface mode
Bridge4(config-if)#switchport	Configure interface as a layer 2 port.
Bridge4(config-if)#bridge-group 4	Associate the interface with bridge group 4.
Bridge4(config-if)#exit	Exit interface mode.

Bridge 3

Bridge3#configure terminal	Enter configure mode.
Bridge3(config)#bridge 3 protocol ieee	Add a bridge (3) to the spanning tree table
Bridge3(config)#interface eth2	Enter interface mode.
Bridge3(config-if)#switchport	Configure interface as a layer 2 port.
Bridge3(config-if)#bridge-group 3	Associate the interface with bridge group 3.
Bridge3(config-if)#exit	Exit interface mode.
Bridge3(config)#interface eth3	Enter interface mode.
Bridge3(config-if)#switchport	Configure interface as a layer 2 port.
Bridge3(config-if)#bridge-group 3	Associate the interface with bridge group 3.
Bridge3(config-if)#exit	Exit interface mode.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change detected
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000525400244323
% 1: Bridge Id 8000525400244323
% 1: last topology change Mon Mar 4 11:40:41 2019
% 1: 20 topology change(s) - last topology change Mon Mar 4 11:40:41 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth1: Designated Port Id 0x8003 - Priority 128 -
% eth1: Root 8000525400244323
% eth1: Designated Bridge 8000525400244323
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
```

```
timer 0
% eth1: forward-transitions 1
% eth1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: bpdu-guard default - Current bpdu-guard off
% eth1: bpdu-filter default - Current bpdu-filter off
% eth1: no root guard configured - Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
% eth1: No auto-edge configured - Current port Auto Edge off
%
% eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
% eth2: Designated Path Cost 0
% eth2: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth2: Designated Port Id 0x8004 - Priority 128 -
% eth2: Root 8000525400244323
% eth2: Designated Bridge 8000525400244323
% eth2: Message Age 0 - Max Age 20
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth2: forward-transitions 1
% eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth2: No portfast configured - Current portfast off
% eth2: bpdu-guard default - Current bpdu-guard off
% eth2: bpdu-filter default - Current bpdu-filter off
% eth2: no root guard configured - Current root guard off
% eth2: Configured Link Type point-to-point - Current point-to-point
Spanning Tree Protocol Configuration
892 © 2020 IP Infusion Inc. Proprietary
% eth2: No auto-edge configured - Current port Auto Edge off
%
% eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
% eth3: Designated Path Cost 0
% eth3: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth3: Designated Port Id 0x8005 - Priority 128 -
% eth3: Root 8000525400244323
% eth3: Designated Bridge 8000525400244323
% eth3: Message Age 0 - Max Age 20
% eth3: Hello Time 2 - Forward Delay 15
% eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth3: forward-transitions 1
% eth3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth3: No portfast configured - Current portfast off
% eth3: bpdu-guard default - Current bpdu-guard off
% eth3: bpdu-filter default - Current bpdu-filter off
% eth3: no root guard configured - Current root guard off
% eth3: Configured Link Type point-to-point - Current point-to-point
% eth3: No auto-edge configured - Current port Auto Edge off
%
% eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
% eth4: Designated Path Cost 0
% eth4: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth4: Designated Port Id 0x8006 - Priority 128 -
```

```
% eth4: Root 8000525400244323
% eth4: Designated Bridge 8000525400244323
% eth4: Message Age 0 - Max Age 20
% eth4: Hello Time 2 - Forward Delay 15
% eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth4: forward-transitions 1
% eth4: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth4: No portfast configured - Current portfast off
% eth4: bpdu-guard default - Current bpdu-guard off
% eth4: bpdu-filter default - Current bpdu-filter off
% eth4: no root guard configured - Current root guard off
% eth4: Configured Link Type point-to-point - Current point-to-point
% eth4: No auto-edge configured - Current port Auto Edge off
%
#
#show spanning-tree interface eth1
% 1: Bridge up - Spanning Tree Enabled - topology change detected
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000525400244323
% 1: Bridge Id 8000525400244323
% 1: last topology change Mon Mar 4 11:40:41 2019
% 1: 20 topology change(s) - last topology change Mon Mar 4 11:40:41 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
Spanning Tree Protocol Configuration
© 2020 IP Infusion Inc. Proprietary 893
% eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth1: Designated Port Id 0x8003 - Priority 128 -
% eth1: Root 8000525400244323
% eth1: Designated Bridge 8000525400244323
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth1: forward-transitions 1
% eth1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: bpdu-guard default - Current bpdu-guard off
% eth1: bpdu-filter default - Current bpdu-filter off
% eth1: no root guard configured - Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
% eth1: No auto-edge configured - Current port Auto Edge off
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled - topology change detected
% 2: Root Path Cost 20000 - Root Port 3 - Bridge Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 2: Root Id 8000525400244323
```

```
% 2: Bridge Id 8000525400d15789
% 2: last topology change Mon Mar 4 11:40:43 2019
% 2: 11 topology change(s) - last topology change Mon Mar 4 11:40:43 2019
% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
% 2: portfast errdisable timeout disabled
% 2: portfast errdisable timeout interval 300 sec
% eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Rootport - State
Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth1: Designated Port Id 0x8003 - Priority 128 -
% eth1: Root 8000525400244323
% eth1: Designated Bridge 8000525400244323
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
% eth1: forward-transitions 1
% eth1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: bpdu-guard default - Current bpdu-guard off
% eth1: bpdu-filter default - Current bpdu-filter off
% eth1: no root guard configured - Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
% eth1: No auto-edge configured - Current port Auto Edge off
%
% eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
Spanning Tree Protocol Configuration
894 © 2020 IP Infusion Inc. Proprietary
% eth2: Designated Path Cost 0
% eth2: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth2: Designated Port Id 0x8004 - Priority 128 -
% eth2: Root 8000525400244323
% eth2: Designated Bridge 8000525400244323
% eth2: Message Age 0 - Max Age 20
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
% eth2: forward-transitions 0
% eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth2: No portfast configured - Current portfast off
% eth2: bpdu-guard default - Current bpdu-guard off
% eth2: bpdu-filter default - Current bpdu-filter off
% eth2: no root guard configured - Current root guard off
% eth2: Configured Link Type point-to-point - Current point-to-point
% eth2: No auto-edge configured - Current port Auto Edge off
%
% eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
% eth3: Designated Path Cost 20000
% eth3: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth3: Designated Port Id 0x8005 - Priority 128 -
% eth3: Root 8000525400244323
% eth3: Designated Bridge 8000525400d15789
% eth3: Message Age 1 - Max Age 20
```

```
% eth3: Hello Time 2 - Forward Delay 15
% eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth3: forward-transitions 1
% eth3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth3: No portfast configured - Current portfast off
% eth3: bpdu-guard default - Current bpdu-guard off
% eth3: bpdu-filter default - Current bpdu-filter off
% eth3: no root guard configured - Current root guard off
% eth3: Configured Link Type point-to-point - Current point-to-point
% eth3: No auto-edge configured - Current port Auto Edge off
%
% eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
% eth4: Designated Path Cost 20000
% eth4: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth4: Designated Port Id 0x8006 - Priority 128 -
% eth4: Root 8000525400244323
% eth4: Designated Bridge 8000525400d15789
% eth4: Message Age 1 - Max Age 20
% eth4: Hello Time 2 - Forward Delay 15
% eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth4: forward-transitions 1
% eth4: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth4: No portfast configured - Current portfast off
% eth4: bpdu-guard default - Current bpdu-guard off
% eth4: bpdu-filter default - Current bpdu-filter off
% eth4: no root guard configured - Current root guard off
% eth4: Configured Link Type point-to-point - Current point-to-point
% eth4: No auto-edge configured - Current port Auto Edge off
%
Spanning Tree Protocol Configuration
© 2020 IP Infusion Inc. Proprietary 895
```

Bridge 3

```
#show spanning-tree
% 3: Bridge up - Spanning Tree Enabled - topology change detected
% 3: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 80005254000835af
% 3: Bridge Id 80005254000835af
% 3: last topology change Mon Mar 4 11:39:11 2019
% 3: 2 topology change(s) - last topology change Mon Mar 4 11:39:11 2019
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
% 3: portfast errdisable timeout disabled
% 3: portfast errdisable timeout interval 300 sec
% eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth1: Designated Port Id 0x8003 - Priority 128 -
% eth1: Root 80005254000835af
% eth1: Designated Bridge 80005254000835af
% eth1: Message Age 0 - Max Age 20
```

```
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth1: forward-transitions 1
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: bpdu-guard default - Current bpdu-guard off
% eth1: bpdu-filter default - Current bpdu-filter off
% eth1: no root guard configured - Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
% eth1: No auto-edge configured - Current port Auto Edge off
%
% eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
% eth2: Designated Path Cost 0
% eth2: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth2: Designated Port Id 0x8004 - Priority 128 -
% eth2: Root 8000254000835af
% eth2: Designated Bridge 80005254000835af
% eth2: Message Age 0 - Max Age 20
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth2: forward-transitions 1
% eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth2: No portfast configured - Current portfast off
% eth2: bpdu-guard default - Current bpdu-guard off
% eth2: bpdu-filter default - Current bpdu-filter off
% eth2: no root guard configured - Current root guard off
% eth2: Configured Link Type point-to-point - Current point-to-point
% eth2: No auto-edge configured - Current port Auto Edge off
%
Spanning Tree Protocol Configuration
896 © 2020 IP Infusion Inc. Proprietary
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled - topology change detected
% 4: Root Path Cost 40000 - Root Port 3 - Bridge Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 4: Root Id 8000525400244323
% 4: Bridge Id 8000525400b83253
% 4: last topology change Mon Mar 4 11:40:40 2019
% 4: 3 topology change(s) - last topology change Mon Mar 4 11:40:40 2019
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
% 4: portfast errdisable timeout disabled
% 4: portfast errdisable timeout interval 300 sec
% eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Rootport - State
Forwarding
% eth1: Designated Path Cost 20000
% eth1: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth1: Designated Port Id 0x8005 - Priority 128 -
% eth1: Root 8000525400244323
% eth1: Designated Bridge 8000525400d15789
```



```
% eth1: Message Age 1 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
% eth1: forward-transitions 1
% eth1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: bpdu-guard default - Current bpdu-guard off
% eth1: bpdu-filter default - Current bpdu-filter off
% eth1: no root guard configured - Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
% eth1: No auto-edge configured - Current port Auto Edge off
%
% eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
% eth2: Designated Path Cost 20000
% eth2: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth2: Designated Port Id 0x8006 - Priority 128 -
% eth2: Root 8000525400244323
% eth2: Designated Bridge 8000525400d15789
% eth2: Message Age 1 - Max Age 20
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
% eth2: forward-transitions 0
% eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth2: No portfast configured - Current portfast off
% eth2: bpdu-guard default - Current bpdu-guard off
% eth2: bpdu-filter default - Current bpdu-filter off
% eth2: no root guard configured - Current root guard off
% eth2: Configured Link Type point-to-point - Current point-to-point
% eth2: No auto-edge configured - Current port Auto Edge off
%
% eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
% eth3: Designated Path Cost 40000
Spanning Tree Protocol Configuration
© 2020 IP Infusion Inc. Proprietary 897
% eth3: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth3: Designated Port Id 0x8005 - Priority 128 -
% eth3: Root 8000525400244323
% eth3: Designated Bridge 8000525400b83253
% eth3: Message Age 2 - Max Age 20
% eth3: Hello Time 2 - Forward Delay 15
% eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth3: forward-transitions 1
% eth3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth3: No portfast configured - Current portfast off
% eth3: bpdu-guard default - Current bpdu-guard off
% eth3: bpdu-filter default - Current bpdu-filter off
% eth3: no root guard configured - Current root guard off
% eth3: Configured Link Type point-to-point - Current point-to-point
% eth3: No auto-edge configured - Current port Auto Edge off
%
% eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
```

```
% eth4: Designated Path Cost 40000
% eth4: Configured Path Cost 20000 - Add type Explicit ref count 1
% eth4: Designated Port Id 0x8006 - Priority 128 -
% eth4: Root 8000525400244323
% eth4: Designated Bridge 8000525400b83253
% eth4: Message Age 2 - Max Age 20
% eth4: Hello Time 2 - Forward Delay 15
% eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth4: forward-transitions 1
% eth4: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth4: No portfast configured - Current portfast off
% eth4: bpdu-guard default - Current bpdu-guard off
% eth4: bpdu-filter default - Current bpdu-filter off
% eth4: no root guard configured - Current root guard off
% eth4: Configured Link Type point-to-point - Current point-to-point
% eth4: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 2 RSTP Configuration

This chapter contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. RSTP provides rapid convergence of a spanning tree. It speeds up the reconfiguration of the tree after a change by using alternate ports.

Topology

The following example is a simple multi-bridge topology.

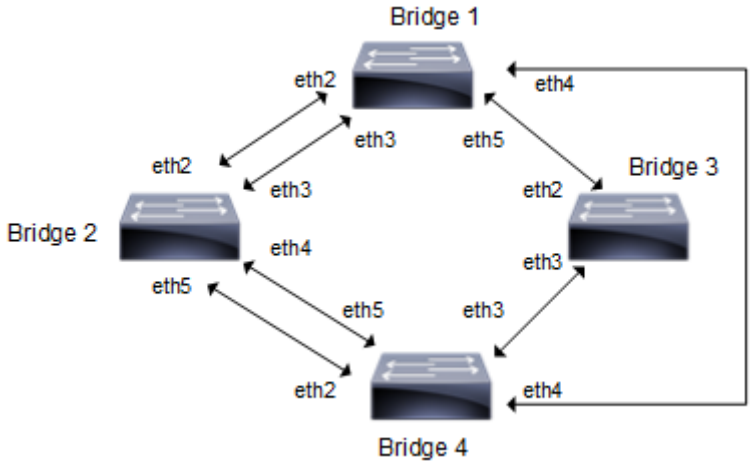


Figure 2-37: RSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol rstp`	Add a bridge (1) to the rapid spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.

`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol rstp`	Add a bridge (2) to the rapid spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol rstp`	Add a bridge `(3)` to the rapid spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol rstp`	Add a bridge `(4)` to the rapid spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group 4.
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 200000 - Root Port 6 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 800052540046f549
% 1: Bridge Id 80005254009cb7e6
% 1: last topology change Tue Aug 11 02:25:01 2020
% 1: 30 topology change(s)  - last topology change Tue Aug 11 02:25:01 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
```

```
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 6
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
```

```
%   eth5: Designated Bridge 800052540065fd8c
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled  - topology change detected
% 2: Root Path Cost 200000 - Root Port 7 -  Bridge Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 2: Root Id 800052540046f549
% 2: Bridge Id 8000525400751db5
% 2: last topology change Tue Aug 11 02:25:00 2020
% 2: 22 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 3
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
```

```
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8007 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Rootport - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 2
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
```

Bridge 3

```
#show spanning-tree
% 3: Bridge up - Spanning Tree Enabled  - topology change detected
% 3: Root Path Cost 200000 - Root Port 5 -  Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 800052540046f549
% 3: Bridge Id 800052540065fd8c
% 3: last topology change Tue Aug 11 02:25:00 2020
% 3: 16 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540065fd8c
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Rootport - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled  - topology change detected
% 4: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 4: Root Id 800052540046f549
% 4: Bridge Id 800052540046f549
% 4: last topology change Tue Aug 11 02:24:58 2020
% 4: 6 topology change(s)  - last topology change Tue Aug 11 02:24:58 2020

% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540046f549
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Path Cost 0
```

```
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 1
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
```

CHAPTER 3 MSTP Configuration

This chapter contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree that is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

Topology

This example gives a simple multi-bridge topology and its configuration.

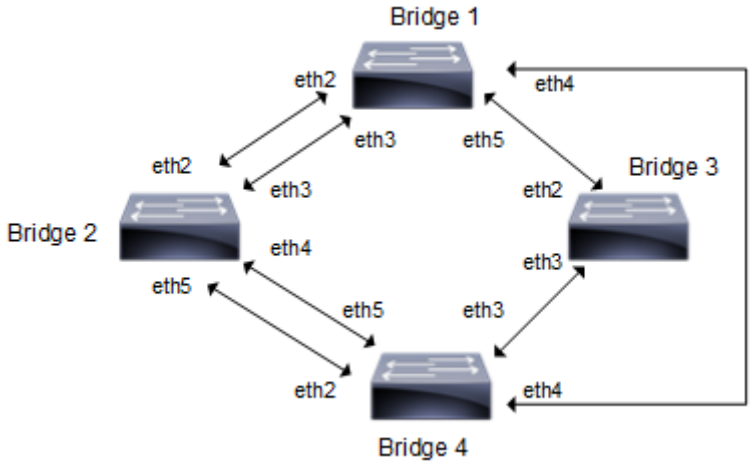


Figure 3-38: MSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#vlan 3 bridge 1 state enable`	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
`Bridge1(config-vlan)#vlan 4 bridge 1 state enable`	Enable the state of VLAN 4 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 1.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable the state of VLAN 5 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 1.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree

`Bridge1(config-mst)#bridge 1 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 3 vlan 3`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 4 vlan 4`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode for eth2
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode for eth3.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode for eth4.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance

`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode for eth5.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol mstp`	Add a bridge (2) to the multiple spanning
`Bridge2(config)#bridge 2 priority 4096`	Assign priority to this bridge.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 2 bridge 2 state enable`	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
`Bridge2(config-vlan)#vlan 3 bridge 2 state enable`	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2
`Bridge2(config-vlan)#vlan 4 bridge 2 state enable`	Enable the state of VLAN 4 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 2
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable the state of VLAN 5 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 2
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree configuration mode
`Bridge2(config-mst)#bridge 2 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode for eth2

`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode for eth3
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode
`Bridge2(config)#interface eth4`	Enter interface mode for eth4
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode for eth5
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2

`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol mstp`	Add a bridge (3) to the multiple spanning tree table
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 2 bridge 3 state enable`	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
`Bridge3(config-vlan)#vlan 3 bridge 3 state enable`	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
`Bridge3(config-vlan)#vlan 4 bridge 3 state enable`	Enable the state of VLAN 4 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 3.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable the state of VLAN 5 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 3.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge3(config-mst)#bridge 3 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode for eth2
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.

`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode for eth3
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol mstp`	Add a bridge (4) to the multiple spanning tree table
`Bridge4(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge4(config-vlan)#vlan 2 bridge 4 state enable`	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
`Bridge4(config-vlan)#vlan 3 bridge 4 state enable`	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
`Bridge4(config-vlan)#vlan 4 bridge 4 state enable`	Enable the state of VLAN 4 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 4.
`Bridge4(config-vlan)#vlan 5 bridge 4 state enable`	Enable the state of VLAN 5 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 4.
`Bridge4(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge4(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge4(config-mst)#bridge 4 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.

`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#exit`	Exit MST Configuration mode.
`Bridge4(config)#interface eth2`	Enter interface mode for eth2
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode for eth3
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode for eth4
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode for eth5
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance

`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail

```
# show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
```

```
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%

% Instance  2:  Vlans: 2
```

```
% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800252540046f549
% 1: MSTI Bridge Id 80025254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800252540046f549
%   eth2: Designated Bridge 80025254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800252540046f549
%   eth3: Designated Bridge 80025254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800252540046f549
%   eth4: Designated Bridge 80025254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800252540046f549
%   eth5: Designated Bridge 80025254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800352540046f549
% 1: MSTI Bridge Id 80035254009cb7e6
```

```
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800352540046f549
%   eth2: Designated Bridge 80035254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800352540046f549
%   eth3: Designated Bridge 80035254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800352540046f549
%   eth4: Designated Bridge 80035254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800352540046f549
%   eth5: Designated Bridge 80035254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  4:  Vlans: 4

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800452540046f549
% 1: MSTI Bridge Id 80045254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
```

```
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800452540046f549
%   eth2: Designated Bridge 80045254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800452540046f549
%   eth3: Designated Bridge 80045254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800452540046f549
%   eth4: Designated Bridge 80045254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800452540046f549
%   eth5: Designated Bridge 80045254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  5:  Vlans: 5

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800552540046f549
% 1: MSTI Bridge Id 80055254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800552540046f549
```

```
%   eth2: Designated Bridge 80055254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800552540046f549
%   eth3: Designated Bridge 80055254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800552540046f549
%   eth4: Designated Bridge 80055254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800552540046f549
%   eth5: Designated Bridge 80055254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

    #show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
```

```
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
```

```
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 4 Disable Spanning Tree Configuration

This chapter describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Topology

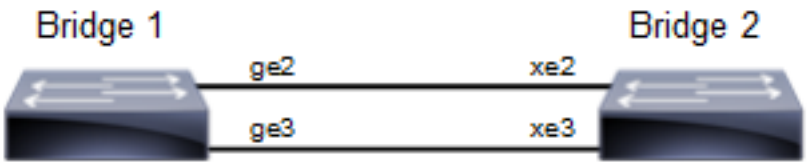


Figure 4-39: Disable Spanning Tree Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Disabling MSTP Configuration

Bridge 1

Disabling MSTP per instance

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP and keeping the ports in forwarding state.

Disabling MSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.

Bridge 2

Disabling MSTP per instance

`Bridge2(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge2(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3

Disabling MSTP globally

`Bridge2(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP.

Disabling MSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify MSTP details with the `show spanning-tree mst detail` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 905 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 9 topology change(s)  - last topology change Thu Nov 17 15:06:17 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: CIST Root 80003417ebfbe9c4
%   ge2: Regional Root 80003417ebfbe9c4
%   ge2: Designated Bridge 80003417ebfbe9c4
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 1
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
```

```
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 2
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5001 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80023417ebfbe9c4
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x838a
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 80023417ebfbe9c4
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800364006ac779a0
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838c
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 800364006ac779a0
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

Verify MSTP configurations when MSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol mstp
```

```
!
```

Verify MSTP configurations when MSTP is disabled globally.

```
#show running-config
!
bridge 1 protocol mstp
no bridge 1 multiple-spanning-tree enable bridge-forward
!
```

Verify MSTP configurations when MSTP instance 2 and 3 is enabled.

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1  instance 2
bridge 1  instance 2 vlan 2
bridge 1  instance 3
bridge 1  instance 3 vlan 3
!
interface xe2
bridge-group 1 instance 2
!
interface xe3
bridge-group 1 instance 3
!
```

- Verify MSTP configurations when MSTP instance 2 is disabled

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1 instance 3
bridge 1 instance 3 vlan 3
!
interface ge3
bridge-group 1 instance 3
!
```

Verify MSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
!
```

Verify MSTP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
```

Verify MSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree mst details` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 908 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 10 topology change(s)  - last topology change Fri Nov 25 21:21:05 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 2
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 3
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
```

```
% 1: MSTI Root Id 800264006ac779a0
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Discarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x8389
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 800264006ac779a0
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5004 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80033417ebfbe9c4
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838b
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 80033417ebfbe9c4
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
```

STP Configuration

Bridge 1

Disabling STP globally

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.

Bridge 2

Disabling STP globally

`Bridge2(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify STP details when stp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 905
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 3 topology changes - last topology change Tue Nov 15 21:33:53 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec

%ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%ge2: Designated Port Id 0x838a - state Forwarding -Priority 128
%ge2: Designated root 80003417ebfbe9c4
%ge2: Designated Bridge 80003417ebfbe9c4
%ge2: Message Age 0 - Max Age 20
%ge2: Hello Time 2 - Forward Delay 15
%ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change  timer0
%ge2: forward-transitions 1
%ge2: No portfast configured – Current  portfast
%ge2: bpdu-guard default- Current bpdu-guard off
%ge2: bpdu-filter default- Current bpdu-filter off
%ge2: no root guard configured- Current root guard off
%ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%ge3: Designated Port Id 0x838b - state Blocked -Priority 128
%ge3: Designated root 80003417ebfbe9c4
%ge3: Designated Bridge 80003417ebfbe9c4
%ge3: Message Age 0 - Max Age 20
%ge3: Hello Time 2 - Forward Delay 15
%ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer0
```

```
%ge3: forward-transitions 0
%ge3: No portfast configured - Currentportfast off
%ge3: bpdu-guarddefault- Current bpdu-guard off
%ge3: bpdu-filter default- Current bpdu-filter off
%ge3: no root guard configured- Current root guard off
%
```

Verify STP configurations when STP is enabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
!
```

Verify STP configurations when STP is disabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
no bridge 1 spanning-tree enable bridge-forward
!
```

Verify STP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 908
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 5 topology changes - last topology change Fri Nov 25 21:15:35 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%   ge2: Designated Port Id 0x838a - state Disabled -Priority 128
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
```

```
%   ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change
timer 23
%   ge2: forward-transitions 2
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%   ge3: Designated Port Id 0x838b - state Forwarding -Priority 128
%   ge3: Designated root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change
timer 23
%   ge3: forward-transitions 2
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
```

RSTP Configuration

Bridge 1

Disabling RSTP globally

`Bridge1(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.

Bridge 2

Disabling RSTP globally

`Bridge2(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify RSTP details when rstp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled- topology change detected
% 1: Root Path Cost 20000 - Root Port 905 -Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Tue Nov 15 21:44:31 2016
% 1: 7 topology change(s)- last topology change Tue Nov 15 21:44:31 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
% ge2: Designated Path Cost 0
% ge2: Configured Path Cost 20000- Add type Explicit ref count 1
% ge2: Designated Port Id 0x838a - Priority 128-
% ge2: Root 80003417ebfbe9c4
% ge2: Designated Bridge 80003417ebfbe9c4
% ge2: Message Age 0 - Max Age 20
% ge2: Hello Time 2 - Forward Delay 15
% ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
% ge2: forward-transitions 1
% ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge2: No portfast configured - Currentportfast off
% ge2: bpdu-guarddefault- Current bpdu-guard off
% ge2: bpdu-filter default- Current bpdu-filter off
% ge2: no root guard configured- Current root guard off
% ge2: Configured Link Type point-to-point - Current point-to-point
% ge2: No auto-edge configured - Current port Auto Edge off
% ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
% ge3: Designated Path Cost 0
% ge3: Configured Path Cost 20000- Add type Explicit ref count 1
% ge3: Designated Port Id 0x838b - Priority 128-
% ge3: Root 80003417ebfbe9c4
% ge3: Designated Bridge 80003417ebfbe9c4
% ge3: Message Age 0 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
```

```
0
% ge3: forward-transitions 2
% ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge3: No portfast configured - Currentportfast off
% ge3: bpdu-guarddefault- Current bpdu-guard off
% ge3: bpdu-filter default- Current bpdu-filter off
% ge3: no root guard configured- Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: No auto-edge configured - Current port Auto Edge off
%
```

Verify RSTP configurations when RSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
!
```

- Verify RSTP configurations when RSTP is disabled globally

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
no bridge 1 rapid-spanning-tree enable bridge-forward
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
```

Verify RSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 20000 - Root Port 908 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Fri Nov 25 21:08:56 2016
% 1: 11 topology change(s)  - last topology change Fri Nov 25 21:08:56 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
```

```
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0x838a - Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
%   ge2: forward-transitions 2
%   ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Path Cost 0
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0x838b - Priority 128  -
%   ge3: Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer
0
%   ge3: forward-transitions 3
%   ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 5 VLAN Configuration

This chapter contains an example for VLAN configuration on trunk port.

Configuring VLAN Tags

Topology

This shows configuring a VLAN bridge with VLAN tags on forwarding frames. Link between Bridge 2 and Bridge 3 is configured with VLAN 5 and VLAN 10. Link between Bridge 2 and Bridge 1 is configured as VLAN 5 and link between Bridge 3 and Bridge 1 is configured as VLAN 10.

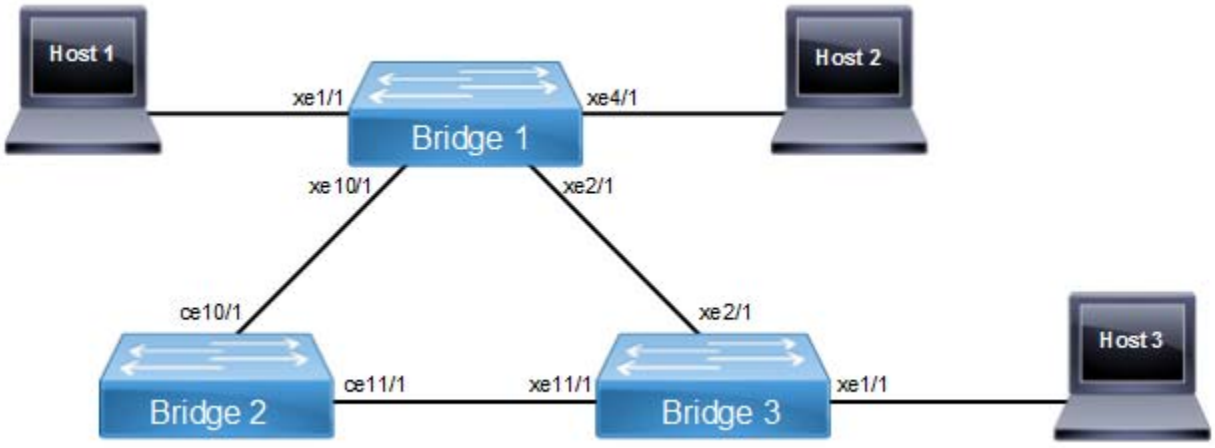


Figure 5-40: VLAN Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configuration mode
`Bridge1(config)#bridge 1 protocol ieee vlan-bridge`	Specify VLAN for bridge 1.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable VLAN (5) on bridge 1.Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#vlan 10 bridge 1 state enable`	Enable VLAN (10) on bridge 1. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#interface xe1/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.

`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe2/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe4/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe10/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee vlan-bridge`	Specify VLAN for bridge 2.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable VLAN (5) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#vlan 10 bridge 2 state enable`	Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#interface ce10/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.

`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge2(config)#interface ce11/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee vlan-bridge`	Specify VLAN for bridge 3.
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable VLAN (5) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#vlan 10 bridge 3 state enable`	Enable VLAN (10) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#interface xe1/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe2/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe11/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.

`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.

Validation

Bridge 1

```
Bridge1#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 1 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 909
% 1: Root Id 8000001823304db6
% 1: Bridge Id 8000001823305244
% 1: 6 topology changes - last topology change Fri Apr 19 12:32:26 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   xe1/1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 - designated
cost 1
%   xe1/1: Designated Port Id 0x8389 - state Forwarding -Priority 128
%   xe1/1: Designated root 8000001823304db6
%   xe1/1: Designated Bridge 8000001823305244
%   xe1/1: Message Age 1 - Max Age 20
%   xe1/1: Hello Time 2 - Forward Delay 15
%   xe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe1/1: forward-transitions 1
%   xe1/1: No portfast configured - Current  portfast off
%   xe1/1: bpdu-guard  default  - Current bpdu-guard off
%   xe1/1: bpdu-filter default  - Current bpdu-filter off
%   xe1/1: no root guard configured     - Current root guard off
%
%   xe2/1: Port Number 909 - Ifindex 5005 - Port Id 0x838d - path cost 1 - designated
cost 0
%   xe2/1: Designated Port Id 0x838d - state Forwarding -Priority 128
%   xe2/1: Designated root 8000001823304db6
%   xe2/1: Designated Bridge 8000001823304db6
%   xe2/1: Message Age 0 - Max Age 20
%   xe2/1: Hello Time 2 - Forward Delay 15
%   xe2/1: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer 0
%   xe2/1: forward-transitions 2
%   xe2/1: No portfast configured - Current  portfast off
%   xe2/1: bpdu-guard  default  - Current bpdu-guard off
%   xe2/1: bpdu-filter default  - Current bpdu-filter off
%   xe2/1: no root guard configured     - Current root guard off
%
```

```
%   xe4/1: Port Number 917 - Ifindex 5013 - Port Id 0x8395 - path cost 4 - designated
cost 1
%   xe4/1: Designated Port Id 0x8395 - state Forwarding -Priority 128
%   xe4/1: Designated root 8000001823304db6
%   xe4/1: Designated Bridge 8000001823305244
%   xe4/1: Message Age 1 - Max Age 20
%   xe4/1: Hello Time 2 - Forward Delay 15
%   xe4/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   xe4/1: forward-transitions 1
%   xe4/1: No portfast configured - Current  portfast off
%   xe4/1: bpdu-guard  default  - Current bpdu-guard off
%   xe4/1: bpdu-filter default  - Current bpdu-filter off
%   xe4/1: no root guard configured     - Current root guard off
%
%   xe10/1: Port Number 941 - Ifindex 5037 - Port Id 0x83ad - path cost 2 - designated
cost 1
%   xe10/1: Designated Port Id 0x83ad - state Forwarding -Priority 128
%   xe10/1: Designated root 8000001823304db6
%   xe10/1: Designated Bridge 8000001823305244
%   xe10/1: Message Age 1 - Max Age 20
%   xe10/1: Hello Time 2 - Forward Delay 15
%   xe10/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe10/1: forward-transitions 2
%   xe10/1: No portfast configured - Current  portfast off
%   xe10/1: bpdu-guard  default  - Current bpdu-guard off
%   xe10/1: bpdu-filter default  - Current bpdu-filter off
%   xe10/1: no root guard configured     - Current root guard off
%
B1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1       0018.23cb.fbbc    1     300
 1         1                   xe10/1      cc37.ab97.37d8    1     300
 1         5                   xe1/1       0000.11bc.5dec    1     300
 1         10                  xe4/1       0000.2d50.205c    1     300
Bridge1#


Bridge1#show vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== =========================
1       1       default          ACTIVE  Success    xe1/1(u) xe2/1(u) xe4/1(u)
                                                    xe10/1(u)
1       5       VLAN0005         ACTIVE  Success    xe1/1(t) xe10/1(t)
1       10      VLAN0010         ACTIVE  Success    xe2/1(t) xe4/1(t)


Bridge1#show bridge
```

```
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1       0018.23cb.fbbc    1     300
 1         1                   xe10/1      cc37.ab97.37d8    1     300
 1         5                   xe1/1       0000.11bc.5dec    1     300
 1         10                  xe4/1       0000.2d50.205c    1     300
Bridge1#
```

Bridge 2

```
Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1      0018.2326.166a    1     300
 2         1                   ce11/1      0018.23cb.fbe0    1     300
 2         1                   ce11/1      cc37.ab97.37d8    1     300
 2         5                   ce10/1      0000.11bc.5dec    1     300


Bridge2#show vlan all bridge 2
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
2       1       default          ACTIVE  Success    ce10/1(u) ce11/1(u)
2       5       VLAN0005         ACTIVE  Success    ce10/1(t) ce11/1(t)
2       10      VLAN0010         ACTIVE  Success    ce10/1(t) ce11/1(t)


Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1      0018.2326.166a    1     300
 2         1                   ce11/1      0018.23cb.fbe0    1     300
 2         1                   ce11/1      cc37.ab97.37d8    1     300
 2         5                   ce10/1      0000.11bc.5dec    1     300
```

Bridge 3

```
Bridge3# show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 3         1                   xe2/1       cc37.ab97.37d8    1     300
 3         5                   xe11/1      0000.11bc.5dec    1     300
 3         10                  xe2/1       0000.2d50.205c    1     300
Bridge3#sh vlan all bridge 3
```

```
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
3       1       default          ACTIVE  Success    xe1/1(u) xe2/1(u) xe11/1(u)
3       5       VLAN0005         ACTIVE  Success    xe1/1(t) xe11/1(t)
3       10      VLAN0010         ACTIVE  Success    xe1/1(t) xe2/1(t)
```

CHAPTER 6 802.1X Configuration

IEEE 802.1x restricts unauthenticated devices from connecting to a switch. Only after authentication is successful, traffic is allowed through the switch.

Topology

In this example, a radius server keeps the client information, validating the identity of the client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client. To configure 802.1x authentication, enable authentication on ports eth1 and eth and specify the radius server IP address and port.

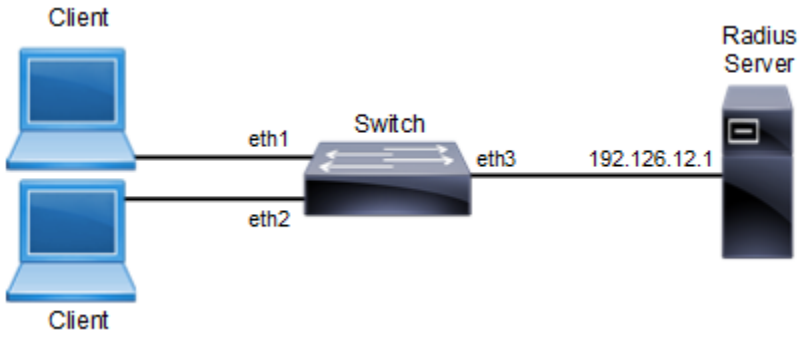


Figure 6-41: 802.1x Topology

Switch Configuration

`Switch#configure terminal`	Enter configure mode.
`Switch(config)#dot1x system-auth-ctrl`	Enable authentication globally.
`Switch(config)#interface eth2`	Enter interface mode.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth2`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#interface eth1`	Enter interface mode.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth1`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#radius-server host 192.126.12.1 auth-port 1812`	Specify the Radius Server address (`192.126.12.1`) and port.
`Switch(config)#radius-server key myKey`	Specify the shared key `myKey` between the radius server and the client.
`Switch(config)#interface eth3`	Enter interface mode.
`Switch(config-if)#ip address 192.126.12.0/24`	Set the IP address on interface `eth3`.

Validation

show dot1x, show dot1x all

```
#show dot1x all
802.1X Port-Based Authentication Enabled
```

```
    RADIUS server address: 192.126.12.1:1812
    Next radius message id: 0
    RADIUS client address: not configured

  802.1X info for interface ge1
    Supplicant address: 0000.0000.0000
    portEnabled: false - portControl: Auto
    portStatus: Unauthorized - currentId: 1
    protocol version: 2
    reAuthenticate: disabled
    reAuthPeriod: 3600
    abort:F fail:F start:F timeout:F success:F
    PAE: state: Connected - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
    BE: state: Invalid - reqCount: 0 - idFromServer: 0
    BE: suppTimeout: 30 - serverTimeout: 30
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false


  #show dot1x
  802.1X Port-Based Authentication Enabled
    RADIUS server address: 192.126.12.1:1812
    Next radius message id: 0
    RADIUS client address: not configured
```

CHAPTER 7 Link Aggregation Configuration

This chapter contains a complete sample Link Aggregation Group configuration.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. Traffic can be load balanced within an LACP trunk group in a controlled manner using the hashing algorithm.The maximum number of physical Ethernet links in a single logical channel depends upon the hardware support.

Note:

- Physical interfaces will inherit the properties of LAG port once it is attached to be part of LAG, irrespective of the configuration present on the physical interface.
- In case of Dynamic LAG, member ports could be moved from one LAG to another LAG, but in case of Static LAG the member port should be unconfigured first then could be aggregated to another Static LAG.
- LAG port should be configured as a switch or router port, before adding member ports into it.

Topology

In Figure 7-42, 3 links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.

Figure 7-42: LACP Topology

Dynamic LAG Configuration

S1

`S1#configure terminal`	Enter configure mode.
`S1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S1(config)#interface po10`	Enter into port channel interface po10.
`S1(config-if)#switchport`	Configure po10 as a layer 2 port.
`S1(config-if)#bridge-group 1`	Associate bridge to an interface.
`S1(config-if)#switchport mode trunk`	Configure port as a trunk.
`S1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S1(config-if)#exit`	Exit interface mode.

`S1(config)#interface eth1`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth2`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth3`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

S2

`S2#configure terminal`	Enter configure mode.
`S2(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S2(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S2(config)#interface po10`	Enter into port channel interface po10.
`S2(config-if)#switchport`	Configure po10 as a layer 2 port.
`S2(config-if)#bridge-group 1`	Associate bridge to an interface.
`S2(config-if)#switchport mode trunk`	Configure port as a trunk.
`S2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth2`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth3`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth4`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

Validation

show etherchannel detail, show etherchannel summary, show running-config interface po10, show running-config interface eth1

```
#show etherchannel detail
% Aggregator po10 7
%  Mac address: 08:00:27:50:6a:9b
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,08-00-27-ab-ea-38,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,08-00-27-f8-3c-30,0x000a
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1
%   Collector max delay: 5

#show etherchannel summary
% Aggregator po10 7
% Admin Key: 0010 - Oper Key 0010
% Aggregator Type: Layer2
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1

#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 channel-group 10 mode active
```

Static LAG Configuration

S1

`S1#configure terminal`	Enter configure mode.
`S1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S1(config)#interface sa10`	Enter into port channel interface sa10.
`S1(config-if)#switchport`	Configure po10 as a layer 2 port.
`S1(config-if)#bridge-group 1`	Associate bridge to an interface.

`S1(config-if)#switchport mode trunk`	Configure port as a trunk.
`S1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth1`	Enter interface mode.
`S1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth2`	Enter interface mode.
`S1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth3`	Enter interface mode.
`S1(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.

S2

`S2#configure terminal`	Enter configure mode.
`S2(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S2(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S2(config)#interface sa10`	Enter into port channel interface po10.
`S2(config-if)#switchport`	Configure po10 as a layer 2 port.
`S2(config-if)#bridge-group 1`	Associate bridge to an interface.
`S2(config-if)#switchport mode trunk`	Configure port as a trunk.
`S2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth2`	Enter interface mode.
`S2(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth3`	Enter interface mode.
`S2(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth4`	Enter interface mode.

S2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S2(config-if)#exit	Exit interface mode.

Validation

```
#show static-channel-group
% Static Aggregator: sa10
% Member status:
   eth1    up
   eth2    up
   eth3    up

#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel load-balance  src-dst-mac

#show running-config interface eth1
!
interface eth1
 static-channel-group 10
```

Static LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

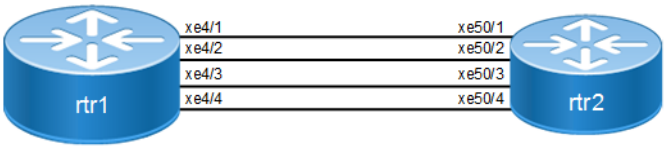


Figure 7-43: LAG Minimum Link

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4(range is 2-32)
`(config-if)#end`	Exit the configure mode

Validation

rtr1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up


#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel load-balance src-dst-mac
 port-channel min-links 4
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
 port-channel min-links 4
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up


Note:When a sa goes down due to the minimum links configured (number of
minimum links is greater than the links aggregated to the sa).
Rtr1:
=====
#OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa10          AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#

Rtr2:
=====

OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa10          AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```

Static-LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

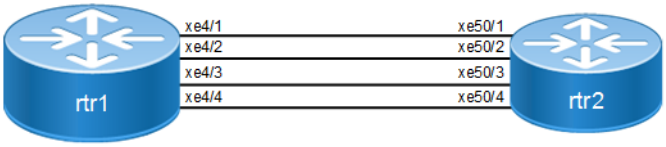


Figure 7-44: LAG Minimum Bandwidth

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#end`	Exit the configure mode

Validation

rtr1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum- 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up



#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel load-balance src-dst-mac
 port-channel min-links 40g
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface sa10
!
interface sa10
```

```
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
 port-channel min-bandwidth 40g
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-bandwidth 40g
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up
```

Note: When sa goes down due to [Total Bandwidth of sa] <[Minimum Bandwidth value Configured]

```
Rtr1:
=====
#OcNOS #sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel Type PVID Mode              Status   Reason Speed
Interface
--------------------------------------------------------------------------------
--
sa10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```

Rtr2:

```
=====

OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
```

```
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


-------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
-------------------------------------------------------------------------------
--
sa10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#

!
```

Dynamic-LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

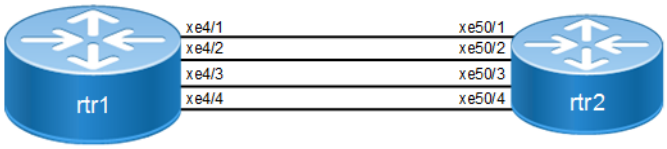


Figure 7-45: LAG Minimum Link

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#end`	Exit the configure mode

Validation

rtr1

```
#sh running-config interface po10

interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
port-channel min-links 4
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-links : 4
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer3
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
-------------------------------------
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface po10
```

```
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
 port-channel min-links 4
!

#show etherchannel

% Lacp Aggregator: po10
% Min-links: 4
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the PO).

```
Rtr1:
#OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode             Status   Reason  Speed
Interface
```

```
    ------------------------------------------------------------------------------
    --
    po10         AGG   1     trunk             down     PD(Min L/B)  0
    OcNOS#


    OcNOS#sh etherchannel
    % Lacp Aggregator: po10
    % Min-links: 4
    % Protocol Down (Min L/B): True
    % Member:
       xe4/1
       xe4/2
       xe4/3
       xe4/4
```

Rtr2:

```
    OcNOS#sh etherchannel
    % Lacp Aggregator: po10
    % Min-links: 4
    % Protocol Down (Min L/B): True
    % Member:
       Xe50/1
       Xe50/2
       Xe50/3
           xe50/4

    OcNOS#sh int brief po100

    Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
           FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
    Port
           CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
    Unknown
           ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
     IA - InActive
           PD(Min L/B) - Protocol Down Min-Links/Bandwidth
           DV - DDM Violation, NA - Not Applicable
           NOM - No operational members, PVID - Port Vlan-id
           Ctl - Control Port (Br-Breakout/Bu-Bundle)
           HD  - ESI Hold Timer Down


    ------------------------------------------------------------------------------
    --
    Port-channel  Type  PVID  Mode              Status   Reason  Speed
    Interface
    ------------------------------------------------------------------------------
    --
    po10         AGG   1     trunk             down     PD(Min L/B)  0
    OcNOS#
```

Dynamic LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

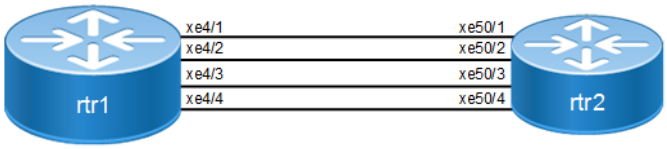


Figure 7-46: LAG Minimum Bandwidth

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#end`	Exit the configure mode

Validation

rtr1

```
#sh running-config interface po10

interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
port-channel min-bandwidth 40g
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe4/1
```

```
   xe4/2
   xe4/3
   xe4/4
-----------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer3
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
-------------------------------------
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mtu 9216
 port-channel load-balance src-dst-mac
 port-channel min-bandwidth 40g
!

#show etherchannel

% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary
```

```
% Aggregator po10 100010
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the [Total bandwidth] < [minimum bandwidth configured]

```
Rtr1:
=====
#OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#


OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4


Rtr2:
=====
OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
```

```
   Xe50/3
       xe50/4

OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```

LACP Minimum-Link, Minimum-Bandwidth Configurations on dynamic, static Channel-Groups with MC-LAG.

Overview

OcNOS allows the configuration of minimum number of the LAG members per LAG group. Both these configurations are meaningful in case the LAG is used for incremental-BW mode. The minimum configuration controls the minimum number of members /bandwidth that must be operationally up / bandwidth available to declare their LAG as operationally UP.

When static/dynamic LAG interface configured with minimum links / minimum bandwidth, the following conditions are to be met:

- Ports which are admin and operational up are considered for min-link.
- The specified minimum number of links should be up.
- Min-link and min-bandwidth cannot co-exist.
- When ports are down due to min-link/min-bandwidth, in show interface brief command output, port down with the corresponding reason code for the failure due to min-link/min-bandwidth.

Minimum Active Members/Bandwidth

The user can specify the minimum number of members that must be operationally up to declare their LAG as operationally UP. Note that this parameter applies to static/dynamic LAG.

```
port-channel min-links <2 - 32>
```

The minimum active member configuration will be allowed to be modified to be greater than the current number of active members. In such configuration, the LAG operational status will become operationally down.

The user can specify the minimum bandwidth, based on the configured value and the ports that satisfy the conditions LAG will be operationally UP. This parameter is applied for static/dynamic LAG.

```
port-channel min-bandwidth BANDWIDTH
```

BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.

When condition fails, the operational state changes to DOWN.

Note: Do not configure minimum-link, Minimum Bandwidth both on TORS and switches at the same time to avoid flaps of MLAG.

Topology

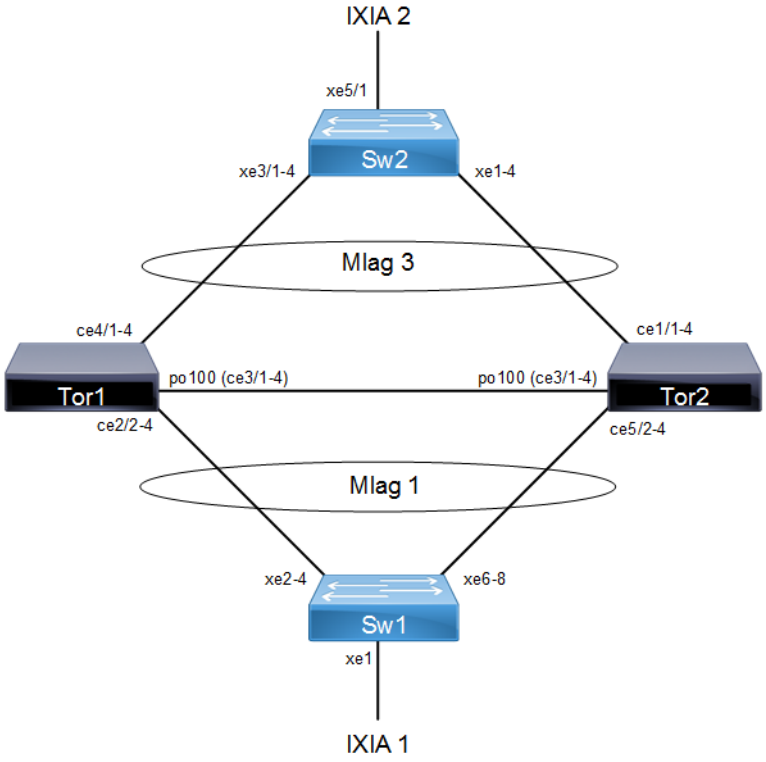


Figure 7-47: MC - LAG Topology

Configuration

TOR1:

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol rstp vlan-bridge end`	Configure bridge type
`configure terminal`	Enter Configure mode
`(config)# vlan database`	Enter vlan database
`(config-vlan)# vlan 600 bridge 1 state enable`	Configure vlans
`(config-if)#end`	
`#configure terminal`	Enter Configure mode.
`(config)#interface mlag1`	Enter Interface mode
`(config-if)# switchport`	Make mlag as layer2 port
`(config-if)# bridge-group 1`	Attach interface to bridge
`(config-if)# switchport mode trunk`	Configure trunk port
`(config-if)# switchport trunk allowed vlan add 600,601,502`	Add interface to vlans
`(config-if)# spanning-tree edgeport`	Configure port as edge port to avoid loops
`(config-if)# spanning-tree bpdu-filter enable`	Enable bpdu filter to avoid loops
`(config-if)#end`	Return to privilege mode
`#configure terminal`	Enter Configure mode.
`(config)#interface mlag3`	Enter Interface mode
`(config-if)# switchport`	Make mlag as layer2 port
`(config-if)# bridge-group 1`	Attach interface to bridge
`(config-if)# switchport mode trunk`	Configure trunk port
`(config-if)# switchport trunk allowed vlan add 600,502`	Add interface to vlans
`(config-if)# spanning-tree edgeport`	Configure port as edge port to avoid loops
`(config-if)# spanning-tree bpdu-filter enable`	Enable bpdu filter to avoid loops
`(config-if)#end`	Return to privilege mode
`#configure terminal`	Enter Configure mode.
`(config)#interface po100`	Enter Interface mode
`(config-if)# switchport`	Make po as layer2 port
`(config-if)# bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)# port-channel load-balance src-dst-mac`	Enable load balance
`(config-if)# mtu 9216`	Configure mtu
`(config-if)#end`	
`#configure terminal`	Enter Configure mode.
`(config)#interface sa1`	Enter Interface mode
`(config-if)# switchport`	Make sa1 as layer2 port

(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce2/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce2/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce2/4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/1	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce4/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce4/2	Enter Interface mode

(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce4/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	
(config)#mcec domain configuration	Enter Multichasis Etherchannel domain configuration mode.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 1	Configure the domain system number
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa/po interface

TOR2

#configure terminal	Enter configure mode.
bridge 1 protocol rstp vlan-bridge end	Configure bridge type

configure terminal	Enter Configure mode.
(config)# vlan database	Enter vlan database
(config-vlan)# vlan 600 bridge 1 state enable	Configure vlans
#configure terminal	Enter Configure mode.
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po(IDL) as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)# mtu 9216	Configure mtu
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make sa1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance

(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make sa3 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/1	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce5/1	Enter Interface mode

(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce5/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface ce5/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#mcec domain configuration	Enter Multichasis Etherchannel domain configuration mode.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 2	Configure the domain system number
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa interface.

SW1

`configure terminal`	Enter Configure mode.
`bridge 1 protocol rstp vlan-bridge`	Configure bridge type
`(config)#vlan database`	Create vlan database
`(config-vlan)#vlan 600,601,502,101,100 bridge 1 state enable`	Create Vlans
`(config-vlan)#end`	Return to privilege mode
`configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter Interface mode
`(config-if)# switchport`	Make xe1 as layer2 port
`(config-if)# bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#spanning-tree edgeport`	Configure port as edgeport
`(config-if)#spanning-tree bpdu-filter enable`	Enable spanning tree bpdu filter
`(config-if)# mtu 9216`	Configure mtu
`(config-if)#end`	Return to privilege mode
`configure terminal`	Enter Configure mode.
`(config)#interface sa1`	Enter Interface mode
`(config-if)# switchport`	Make xe1 as layer2 port
`(config-if)# bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan add 100,101,300,401,402`	Enable all VLAN identifiers on this interface.
`(config-if)# port-channel load-balance src-dst-mac`	Enable load balance
`(config-if)#spanning-tree edgeport`	Configure port as edgeport
`(config-if)#spanning-tree bpdu-filter enable`	Enable spanning tree bpdu filter
`(config-if)# mtu 9216`	Configure mtu
`(config-if)#end`	Return to privilege mode
`#configure terminal`	Enter Configure mode.
`(config)#interface xe2`	Enter Interface mode
`(config-if)# static-channel-group 1`	Add interface to sa1
`(config-if)#end`	Return to privilege mode
`#configure terminal`	Enter Configure mode.
`(config)#interface xe3`	Enter Interface mode
`(config-if)# static-channel-group 1`	Add interface to sa1
`(config-if)#end`	Return to privilege mode
`#configure terminal`	Enter Configure mode.
`(config)#interface xe4`	Enter Interface mode

(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe6	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe7	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe8	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#end	Return to privilege mode

SW2

configure terminal	Enter Configure mode.
bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)#vlan database	Create vlan database
(config-vlan)#vlan 600,601,502,101,100 bridge 1 state enable	Create vlans
(config-vlan)#end	Return to privilege mode
configure terminal	Enter Configure mode.
(config)#interface xe5/1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#end	Return to privilege mode
configure terminal	Enter Configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,401,402,600,502	Enable all VLAN identifiers on this interface.

(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe3/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe3/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe3/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#interface xe1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#end	Return to privilege mode

This configuration is applicable for the dynamic LAG with MC-LAG topology except dynamic LAG interface creations, which needs to be referred from the dynamic LAG configurations given above.

Validation Commands

sh int brief sa [id], sh int brief po [id], sh mlag-domain summary, sh static-channel-group <sa id>, <sh etherchannel>, sh running-config interface sa [id], <sh etherchannel summary>.

When sa or po goes down due to min-link or min-bandwidth not satisfied, below validations to be done:

rtr2

```
#sh int brief sa1
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
```

```
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa1           AGG   1     trunk             down     PD(Min L/B)  0

#
#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po100         AGG   1     trunk             down     PD(Min L/B)  0

#
#sh etherchannel
% Lacp Aggregator: po100
% Min-Bandwidth : 40g
% Protocol Down (Min L/B) : True
% Member:
   ce3/1
   ce3/2
   ce3/3
   ce3/4
-----------------------------------
% Lacp Aggregator: po200
% Member:
   ce29/1
```

```
   ce29/2
-------------------------------------
% Lacp Aggregator: sa1
% Min-links : 3
% Protocol Down (Min L/B): True
% Member:
   ce2/2
   ce2/3
   ce2/4
-------------------------------------
% Lacp Aggregator: sa3
% Member:
   ce4/1
   ce4/2
   ce4/3
#
#sh running-config interface sa1
!
interface sa1
 switchport
 port-channel load-balance src-dst-mac
 port-channel min-links 3
 mlag 1
!

#sh static-channel-group 1
 Static Aggregator: sa1
 Minimum-Links 3
 Member Status
  ce2/2          down
  ce2/3          down
  ce2/4          down
#
#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce3/1 (5057) sync: 0
     Link: ce3/2 (5058) sync: 0
     Link: ce3/3 (5059) sync: 0
     Link: ce3/4 (5060) sync: 0
-------------------------------------
```

LACP Force-Up

In an aggregated environment, there are some parameters that are set for member ports in lag. Whenever the parameters are set and conditions are satisfied, the port channel will be in SYNC. If force-up mode is enabled for the member port, the port channel will always be in SYNC even if the parameters are not set i.e. the traffic will not be affected and the port channel will never go down.

LACP force-up with Dynamic LAG

Topology

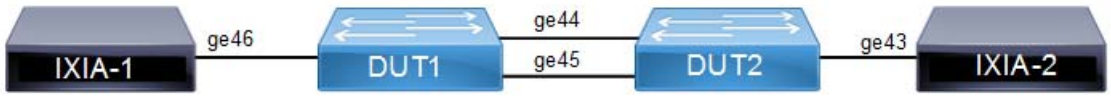


Figure 7-48: LACP force-up with Dynamic LAG

DUT1

`#configure terminal`	Enter configure mode.
`(config)#hostname DUT1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface ge46`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`(config)#interface po1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed vlan all for the hybrid mode
`(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`(config)#interface ge44`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Adding interface to channel-group 1
`(config)#interface ge45`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Adding interface to channel-group 1

DUT2

`#configure terminal`	Enter configure mode.
`(config)#hostname DUT2`	Configure host name
`(config)#bridge 1 protocol provider-rstp edge`	Create provider rstp edge bridge
`(config)#vlan database`	Enter vlan database mode

(config-vlan)#vlan 2-100 type customer bridge 1 state enable	Configure customer VLAN for the bridge
(config-vlan)#vlan 100 type service point-point bridge 1 state enable	Configure service VLAN for the bridge
(config)#exit	Exit vlan database mode
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config)#cvlan 2-100 svlan 100	Mapping cvlan to svlan
(config)#interface ge43	Enter interface mode
(config-if)#switchport	Make interface as Switchport
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)# switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface with bridge group 1
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on lag interface
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1

Send L2 traffic with incremental source mac of 1000 and with VLAN 100 from IXIA1 and with incremental source mac of 1000 and with SVLAN 100(TPID 0x88a8), CVLAN 100 from IXIA2.

Validation

DUT1

```
DUT1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

DUT1#show etherchannel summary
```

```
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5043) sync: 1
     Link: ge45 (5046) sync: 1

DUT1#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ge44                363.65         710252        772.76         1420506
 ge45                363.63         710222        0.00           0
 ge46                772.77         1420525       727.31         1420526
 po1                 728.56         1422971       774.09         1422966

DUT2#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

DUT2#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ge43                774.26         1423267       784.17         1361411
 ge44                774.26         1423268       364.36         711634
 ge45                0.00           0             364.36         711634
 po1                 774.26         1423267       728.71         1423267

DUT2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 1
     Link: ge45 (5022) sync: 1

On server side (DUT1) to make LAG down you can unconfigure the channel-group 1
configurations and verify force-up is getting enabled in DUT2.
To simulate the force-up
```

DUT1(config)#interface ge44	Enter interface mode.
DUT1(config-if)#no channel-group	Removing channel-group configurations from interface.
DUT1(config)#interface ge45	Enter interface mode.
DUT1(config-if)#no channel-group	Removing channel-group configurations from interface.

DUT2

```
DUT2#show interface brief | include po1
po1           AGG   1     customer-edge     up       none    1g
```

```
DUT2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 0 (force-up)
     Link: ge45 (5022) sync: 0

DUT2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: b8:6a:97:4d:65:d5
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,b8-6a-97-28-a5-c0,0x0001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge44 (5020) sync: 0 (force-up)
    Link: ge45 (5022) sync: 0
  Collector max delay: 5

To forward traffic from ge44 of DUT1
```

`DUT1(config)#interface ge44`	Enter interface mode.
`DUT1(config-if)#switchport`	Make the interface as switch port.
`DUT1(config-if)#bridge-group 1`	Associate the interface to bridge.
`DUT1(config-if)#switchport mode hybrid`	Configure the mode as hybrid.
`DUT1(config-if)#switchport hybrid allowed vlan all`	Configure allowed vlan all for the hybrid mode.
`DUT1(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds.

```
DUT2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge43                774.25         1423257       784.17         1361400
 ge44                774.25         1423258       728.71         1423257
 ge45                0.00           0             0.00           0
 po1                 774.25         1423247       728.70         1423245
 DUT2#
DUT1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge44                657.67         1284505       640.77         1177884
 ge45                0.00           0             0.00           0
 ge46                772.71         1420426       603.08         1177886
```

CHAPTER 8 MC-LAG Configuration

This chapter contains a complete example of Multi-Chassis Link Aggregation (MC-LAG) configuration.

MC-LAG expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node running Link aggregation. As a result even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: MC-LAG is only compatible with VPWS.

Note: MC-LAG is supported only in Active-Standby mode.

Note: All MC-LAG nodes must have the same MAC table size – as specified by each node's switching ASIC forwarding profile limit.

Topology

In the below example Switch 1 and Switch 2 forms a MLAG domain.

As shown in Figure 8-49, switch 1 and switch 2 are a single logical switches to switch 3 and switch 4. Even if either switch 1 or switch 2 is down, there exists a path to reach other destinations.

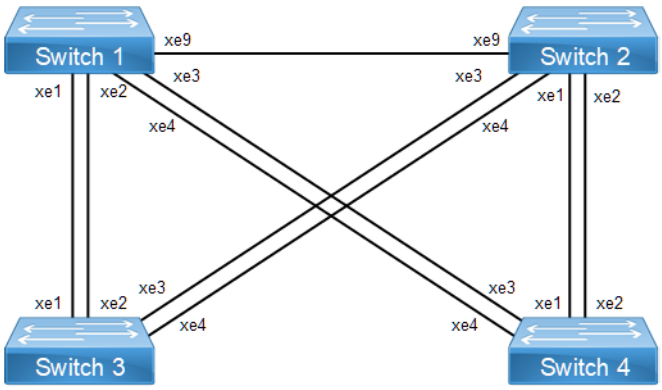


Figure 8-49: MC-LAG Topology

Configuration

Switch 1

`#configure terminal`	Enter configure mode.
`(config)#service-template VLAN2`	Configure a service template for L2VPN.
`(config-svc)# match outer-vlan 2`	Match outer VLAN 2 for L2VPN.
`(config)#service-template VLAN3`	Configure a service template for L2VPN
`(config-svc)# match outer-vlan 3`	Match outer VLAN 3 for L2VPN.
`(config-svc)#exit`	Exit the service template mode.
`(config)#mpls l2-circuit VLAN2 2 10.1.1.1`	Configure the VPWS instance.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2

(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the domain address for the mlag domain.
(config-mcec-domain)#intra-domain link xe9	Configure the intra domain link between mlag domain.
(config-mcec-domain)#domain-system-number 1	Configure the number to identify the node in a domain.
(config-mcec-domain)#exit	Exit MCEC mode.
(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Enable mlag group number.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#mlag 2	Enable mlag group number.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter Interface mode
(config-if)#mpls-l2-circuit VLAN2 service-template VLAN2	Attach VPWS VLAN2 to interface P01.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter Interface mode
(config-if)#mpls-l2-circuit VLAN2 service-template VLAN2	Attach VPWS VLAN2 to interface P01.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter Interface mode

(config-if)#mpls-l2-circuit VLAN3 service-template VLAN3	Attach VPWS VLAN2 to interface P01.
(config-if)#exit	Exit interface mode.

Switch 2

#configure terminal	Enter configure mode.
(config)#service-template VLAN2	Configure a service template for L2VPN
(config)# match outer-vlan 2	Match outer VLAN2 for L2VPN
(config)#service-template VLAN3	Configure a service template for L2VPN
(config)# match outer-vlan 3	Match outer VLAN3 for L2VPN
(config-svc)#exit	Exit the service template mode
(config)#mpls l2-circuit VLAN2 2 10.1.1.1	Configure VPWS instance
(config)# mpls l2-circuit VLAN2 2 10.1.1.1	Configure VPWS instance
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 2 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#channel-group 2 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the domain address for the mlag domain.

(config-mcec-domain)#intra-domain link xe49	Configure the Intra domain link between mlag domain.
(config-mcec-domain)#domain-system-number 2	Configure the number to identify the node in domain.
(config-mcec-domain)#exit	Exit MCEC mode
(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Enable mlag group number.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#mlag 2	Enable mlag group number.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter Interface mode
(config-if)#mpls-l2-circuit VLAN3 service-template VLAN3	Attach VPWS VLAN3 to interface P01.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#mpls-l2-circuit VLAN2 service-template VLAN2	Attach VPWS VLAN2 to interface P01.
(config-if)#exit	Exit interface mode.

Switch 3

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.

(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

Switch 4

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 3 bridge 1 state enable	Create VLAN 3.
(config)#interface xe9	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

(config)#interface xe57	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

Validation

Switch 1

```
#sh mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 1000
Intra Domain Interface         : xe49

Hello RCV State                : Current
Hello Periodic Timer State     : Fast Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
```

```
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC

MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 16386
  Oper Key                    : 16386
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32770
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC

#sh etherchannel summary
% Aggregator po1 0
% Admin Key: 16385 - Oper Key 16385
%   Link: xe57 (5057) sync: 1
%   Link: xe58 (5058) sync: 1
% Aggregator po2 0
% Admin Key: 16386 - Oper Key 16386
%   Link: xe9 (5009) sync: 1
%   Link: xe10 (5010) sync: 1

#sh mlag 1 detail

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC

sh mcec statistics

Unknown MCCPDU received on the system           : 0

-------------------------------------
IDP xe49
-------------------------------------
   Valid RX Hello PDUs                          : 398
   Valid TX Hello PDUs                          : 417
   Valid RX Info PDUs                           : 16
   Valid TX Info PDUs                           : 6

   Valid RX Mac Sync PDUs                       : 3
```

```
   Valid TX Mac Sync PDUs                        : 4

MLAG 1
  Valid RX Info PDUs                             : 8
  Valid TX Info PDUs                             : 3

MLAG 2
  Valid RX Info PDUs                             : 8
  Valid TX Info PDUs                             : 3
sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 1000
Intra Domain Interface          : xe49
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC


MLAG-2
  Mapped Aggregator           : po2
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
```

CHAPTER 9 PW Redundancy with MC-LAG Configuration

This chapter contains configuration for Pseudowire Redundancy with MC-LAG (Active and Standby). It also provides an overview of Pseudowire concepts.

In a single-segment pseudowire (SS-PW) application, the Packet Switched Network (PSN) layer usually provides protection for the PW. One way is by using an RSVP LSP with Fast Reroute (FRR) backup; another way is an end-to-end backup LSP. However, there are some applications where the backup PW terminates on a different target PE node, so PSN protection methods cannot protect against failure of either the target Provider Edge (PE) node or a remote Access Circuit (AC). It is also important for an operator that a particular PW is preferred. For example, the one with the least latency.

PW redundancy supports Label Distribution Protocol (LDP) PW. In the case of PW applications, the PSN layer can provide the protection for PW. Occasionally, a TE LSP signaled by RSVP-TE can be used as a PSN tunnel for a PW. In this scenario, TE can provide FRR to protect the end-to-end LSP in the PSN layer.

FRR-based protection schemes cannot protect against failure of PE nodes and access circuits. However, PW redundancy can protect against these failures.

MC-LAG expands the concept of link aggregation so that it provides node-level redundancy by allowing two nodes to share a common LAG endpoint. This gives PE redundancy for CE node.

CE devices can be connected to two PE nodes for PE-node-level redundancy using MC-LAG.

End-to-End traffic flow decision will take by MC-LAG Active node not by PW-Redundancy node.

Topology

In the below example PE1 and PE2 forms a MLAG domain.

As shown in Figure 9-50, PE1 and PE2 are a single logical switches to P3 and P4. Even if either PE1 or PE2 is down, there exists a path to reach other destinations.

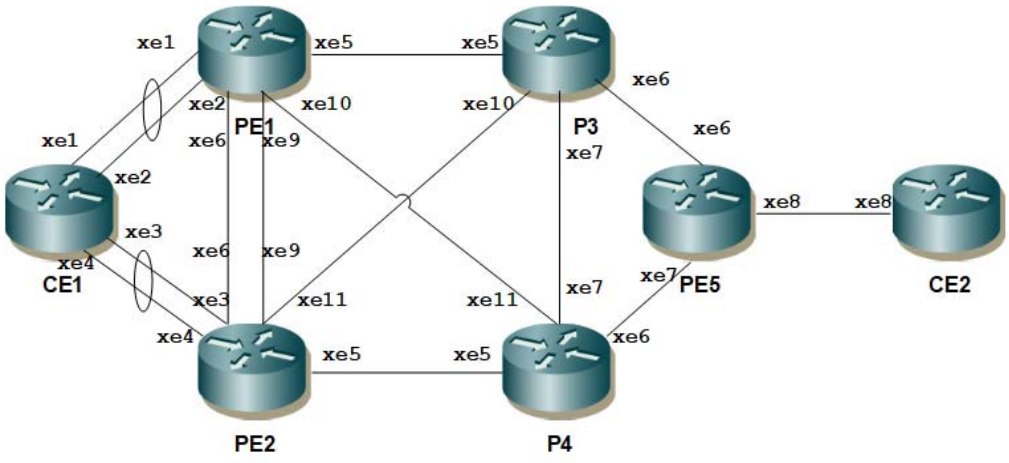


Figure 9-50: MC-LAG Topology

Uplink Interface and OSPF Configuration

PE1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 35.35.35.35/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.35.48.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe9`	Enter interface mode.
`(config-if)# ip address 10.35.33.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe10`	Enter interface mode.
`(config-if)# ip address 10.35.49.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Enter the Router mode for OSPF.
`(config-router)#ospf router-id 35.35.35.35`	Configure OSPF router ID.
`(config-router)# bfd all-interfaces`	Configure BFD on OSPF.
`(config-router)#network 10.35.48.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.35.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.35.33.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#exit`	Exit router mode.

PE2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 33.33.33.33/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.33.49.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe9`	Enter interface mode.
`(config-if)# ip address 10.35.33.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe11`	Enter interface mode.

(config-if)# ip address 10.33.48.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 33.33.33.33	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.33.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.33.49.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.35.33.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#exit	Exit router mode

P3

#configure terminal	Enter configure mode.
(config)#interface lo	Configure the Loopback interface.
(config-if)# ip address 48.48.48.48/32 secondary	Set the IP address of the loopback interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe5	Enter interface mode.
(config-if)# ip address 10.35.48.2/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe6	Enter interface mode.
(config-if)# ip address 10.48.32.1/30	Set the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# ip address 10.48.49.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# ip address 10.33.48.2/30	Set the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 48.48.48.48	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.35.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.48.49.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.48.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.33.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#exit	Exit router mode

P4

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 49.49.49.49/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.33.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# ip address 10.49.32.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe7`	Enter interface mode.
`(config-if)# ip address 10.48.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe10`	Enter interface mode.
`(config-if)# ip address 10.35.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Enter the Router mode for OSPF.
`(config-router)#ospf router-id 49.49.49.49`	Configure OSPF router ID.
`(config-router)# bfd all-interfaces`	Configure BFD on OSPF.
`(config-router)#network 10.35.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.48.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.49.32.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.33.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-if)#exit`	Exit interface mode.

P5

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 32.32.32.32/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# ip address 10.48.32.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.

(config)# interface xe7	Enter interface mode.
(config-if)# ip address 10.49.32.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 32.32.32.32	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.48.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.49.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-if)#exit	Exit interface mode.

RSVP Global Configuration

PE1

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the router mode for RSVP.
(config-router)# no-php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe10	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

PE2

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no-php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface

(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface.
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

P3

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no-php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe6	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

P4

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no-php	Configure no PHP
(config-router)#exit	Exit router mode.

(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe6	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe10	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

P5

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no-php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe6	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

RSVP-LSP Configuration

PE1

#configure terminal	Enter configure mode.
(config)# rsvp-path 35-to-32 mpls	Configure RSVP-Path PE5
(config-path)# 10.35.48.2 strict	Configure Strict hop

(config-path)# 10.48.32.2 strict	Configure Strict hop
(config-path)#exit	Exit RSVP-Path mode
(config)#rsvp-trunk 35-to-32	Configure RSVP-Trunk to PE5
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection
(config-trunk)# primary path 35-to-32	Set RSVP path.
(config-trunk)# to 32.32.32.32	Configure RSVP-LSP destination IP address
(config-trunk)#exit	Exit RSVP-Trunk mode

PE2

#configure terminal	Enter configure mode.
(config)# rsvp-path 33-to-32 mpls	Configure RSVP-Path to PE5
(config-path)# 10.33.49.2 strict	Configure Strict hop
(config-path)# 10.49.32.2 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)#rsvp-trunk 33-to-32	Configure RSVP trunk to PE5.
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection
(config-trunk)# primary path 33-to-32	Set RSVP path.
(config-trunk)# to 32.32.32.32	Configure RSVP LSP destination IP address.
(config-trunk)#exit	Exit RSVP-Trunk mode

PE5

#configure terminal	Enter configure mode.
(config)# rsvp-path 32-to-35 mpls	Configure RSVP path to PE1
(config-path)# 10.48.32.1 strict	Configure Strict hop
(config-path)# 10.35.48.1 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)# rsvp-path 32-to-33 mpls	Configure RSVP path to PE2
(config-path)# 10.49.32.1 strict	Configure Strict hop
(config-path)# 10.33.49.1 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)#rsvp-trunk 32-to-35	Configure RSVP trunk.to PE1.
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection

(config-trunk)# primary path 32-to-35	Set RSVP path
(config-trunk)# to 33.33.33.33	Configure RSVP-LSP destination IP address.
(config-trunk)#exit	Exit RSVP trunk mode

T-LDP Configuration

PE1

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 35.35.35.35	Configure LDP router ID.
(config-router)# pw-status-tlv	Set PW status TLV
(config-router)# no multicast-hellos	Disable Multicast hellos
(config-router)# targeted-peer ipv4 32.32.32.32	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe5	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe10	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

PE2

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 33.33.33.33	Configure LDP router ID
(config-router)# pw-status-tlv	Set PW status TLV.
(config-router)# no multicast-hellos	Disable multicast hellos
(config-router)# targeted-peer ipv4 32.32.32.32	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe5	Enter interface mode.

(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

PE5

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 32.32.32.32	Configure LDP router ID
(config-router)# pw-status-tlv	Set PW status TLV
(config-router)# no multicast-hellos	Disable multicast hellos
(config-router)# targeted-peer ipv4	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)# targeted-peer ipv4 33.33.33.33	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe6	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

MC-LAG Configuration

CE1

#configure terminal	Enter configure mode.
(config)#interface po1	Configure the LAG interface
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.

(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.

PE1

#configure terminal	Enter configure mode.
(config)#mcec domain configuration	Configure MC-LAG global.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 1	Configure Domain System number.
(config-mcec-domain)# intra-domain-link xe6	Configure IDL link.
(config-mcec-domain)#exit	Exit MC-LAG global mode.
(config)#interface po1	Configure the LAG interface
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface po1	Configure the LAG interface
(config-if)# mlag 1	Configure MC-LAG domain to LAG interface
(config-if)#exit	Exit interface mode.

PE2

`#configure terminal`	Enter configure mode.
`(config)#mcec domain configuration`	Configure MC-LAG global
`(config-mcec-domain)# domain-address 1111.2222.3333`	Configure the Domain address
`(config-mcec-domain)# domain-system-number 2`	Configure Domain System number.
`(config-mcec-domain)# intra-domain-link xe6`	Configure IDL link.
`(config-mcec-domain)#exit`	Exit MC-LAG global mode.
`(config)#interface po1`	Configure the LAG interface
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
`(config-if)#exit`	Exit interface mode.
`(config)#interface po1`	Configure the LAG interface
`(config-if)# mlag 1`	Configure MC-LAG domain to LAG interface
`(config-if)#exit`	Exit interface mode.

VPWS PW Redundancy Configuration

PE1

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC1 1001 32.32.32.32`	Configure VPWS to PE5
`(config)#int po1`	Enter interface mode
`(config-if)#mpls-l2-circuit VC1 service-template S-00-00-10`	Attach VPWS to AC interface.
`(config-if)#exit`	Exit interface

PE2

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC2 1002 32.32.32.32`	Configure VPWS to PE5
`(config)#int po1`	Enter interface mode
`(config-if)#mpls-l2-circuit VC2 service-template S-00-00-10`	Attach VPWS to AC interface.
`(config-if)#exit`	Exit interface

PE5

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC1 1001`	Configure VPWS to PE1
`(config)# mpls l2-circuit VC2 1002 33.33.33.33`	Configure VPWS to PE2
`(config)#int xe8`	Enter interface mode
`(config-if)# switchport`	Switch to Layer 2 mode.
`(config-if)#mpls-l2-circuit VC1 service-template S-00-00-10`	Attach Primary VPWS to AC interface.
`(config-if)# mpls-l2-circuit VC2 service-template S-00-00-10 secondary`	Attach Secondary VPWS to AC interface.
`(config-if)#exit`	Exit interface

Validation

To see detail information about the MC-LAG, use the following command:

```
MC_LAG Active node
PE1#sh mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 1
```

```
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : xe12

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Active


MC-LAG Standby node

PE2#sh mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 2
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : xe12

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 32769
```



```
  Oper Key                      : 32769
  Physical properties Digest    : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a

  Neigh Admin Key               : 16385
  Neigh Physical Digest         : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Info RCV State                : Current
  Info Periodic Time State      : Standby
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Standby
```

To see summary information about the MC-LAG, use the following command:

```
Mc-LAG active node
PE1#sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe12
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Total Bandwidth               : 20g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Active

Standby node
PE2#sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe12
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------
```

```
MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Total Bandwidth              : 20g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
      Current Mlag state           : Standby
```

To see summary information about the Virtual Circuits, use the following command:

```
#show mpls vc-table
The samples below show summary information about the just-configured four
virtual circuits.
PE1#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1001        N/A      N/A            po1           xe14          24960
24324         32.32.32.32     Active
PE1#

PE2#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1002        N/A      N/A            po1           xe14          24961
24323         32.32.32.32     Inactive
PE2#

PE5#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1001        N/A      N/A            xe23          xe12          24986
24322         35.35.35.35     Active
1002        N/A      N/A            xe23          xe12          24968
24320         33.33.33.33     Inactive
PE5#
```

To view detailed configuration information about the L2 Virtual Circuits, including LDP PW status, use the following command:

```
PE1#sh ldp mpls-l2-circuit 1001 detail
vcid: 1001  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 32.32.32.32, Peer LDP Ident: 32.32.32.32
Local label: 24986, remote label: 24960
Access IF: po1, Network IF: xe13
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Forwarding
  Active
Remote PW Status :
  Forwarding
  Active
```

```
PE2#sh ldp mpls-l2-circuit 1002 detail
vcid: 1002  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 32.32.32.32, Peer LDP Ident: 32.32.32.32
Local label: 24968, remote label: 24961
Access IF: po1, Network IF: xe14
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Not Forwarding
  Ingress AC Receive Fault
  Egress AC Transmit Fault
Remote PW Status :
  Not Forwarding
  Standby

PE5#sh ldp mpls-l2-circuit 1001 detail
vcid: 1001  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 35.35.35.35, Peer LDP Ident: 35.35.35.35
Local label: 24960, remote label: 24986
Access IF: xe23, Network IF: xe14
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Forwarding
  Active
Remote PW Status :
  Forwarding
  Active

PE5#sh ldp mpls-l2-circuit 1002 detail
vcid: 1002  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 33.33.33.33, Peer LDP Ident: 33.33.33.33
Local label: 24961, remote label: 24968
Access IF: xe23, Network IF: xe12
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Not Forwarding
  Standby
Remote PW Status :
  Not Forwarding
  Ingress AC Receive Fault
  Egress AC Transmit Fault
```

CHAPTER 10 Traffic Mirroring Configuration

This chapter contains a sample local and remote switched port analyzer feature configuration.

SPAN Overview

Switched Port Analyzer (SPAN) refers to selecting network traffic for analysis by a network analyzer. SPAN feature is introduced on switches as the switch forwards traffic that is destined for a MAC address directly to the corresponding port leaving no scope to analyze the traffic.

SPAN monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. Source port can be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis

SPAN is originally referred to port mirroring or port monitoring where all the network traffic on the source port is mirrored to destination port. Port mirroring has three subdivisions.

- Ingress mirroring: Traffic received on the source port will be monitored
- Egress mirroring: Traffic transmitted from the source port will be monitored
- Ingress and egress mirroring: Both received and transmitted traffic on the source port will be monitored.

With enhancements to SPAN, mirroring can be classified into three categories.

Port Mirroring

In port mirroring, source will be a port which could be a physical interface or a port channel. All the traffic on the source port will be mirrored to destination port. Either traffic received on the source port or traffic transmitted from the source port or both can be monitored.

VLAN Mirroring

In VLAN mirroring, the source is a VLAN identifier and the traffic received on all ports with the VLAN identifier matching source VLAN identifier are mirrored to destination port.

Rule Based Mirroring

In rule based mirroring, there is a set of matching criteria for the ingress traffic such as matching destination MAC address, matching frame type, and so on. The traffic matching the rules is mirrored to the destination port

Topology

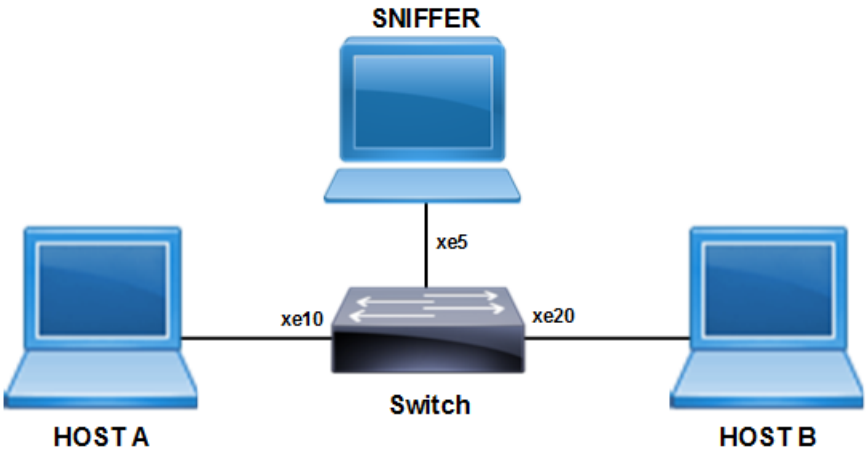


Figure 10-51: SPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

Note: Use the below command for port mirroring.

```
mirror interface <if-name> direction both|receive|transmit
```

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.

(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Note: Use the below command for validate the mirroring.

```
show mirror interface <if-name>
```

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source interface xe10 both
 destination interface xe5
 no shut

#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            : xe10
    rx            : xe10
    both          : xe10
source VLANs      :
    rx            :
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring

This example shows detailed configuration of VLAN with rule based mirroring.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs
(config)#interface xe10	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source vlan 101	Configure source VLAN to be mirrored
(config-monitor)# filter src-mac host 0000.0000.0005	Configure the rule to match the source MAC
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source vlan 101
 destination interface xe5
```

```
 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            :
    rx            :
    both          :
source VLANs      :
    rx            : 101
destination ports : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

RSPAN Overview

When several switches need to be analyzed with a single centralized sniffer, remote switched port analyzer (RSPAN) is used. In RSPAN, all the mirrored traffic will be tagged with a RSPAN VLAN ID and forwarded to remote destination via a port called reflector port. Reflector port will have the same characteristics of a local destination port. RSPAN VLAN ID will be a dedicated VLAN for the monitoring purpose and will not participate in bridging. RSPAN destination switch will strip the RSPAN VLAN tag and send it the sniffer for analysis. RSPAN will have the same sub-categories as SPAN except that the mirrored traffic will be tagged with RSPAN VLAN header and forwarded to destination switch for analysis.

Topology

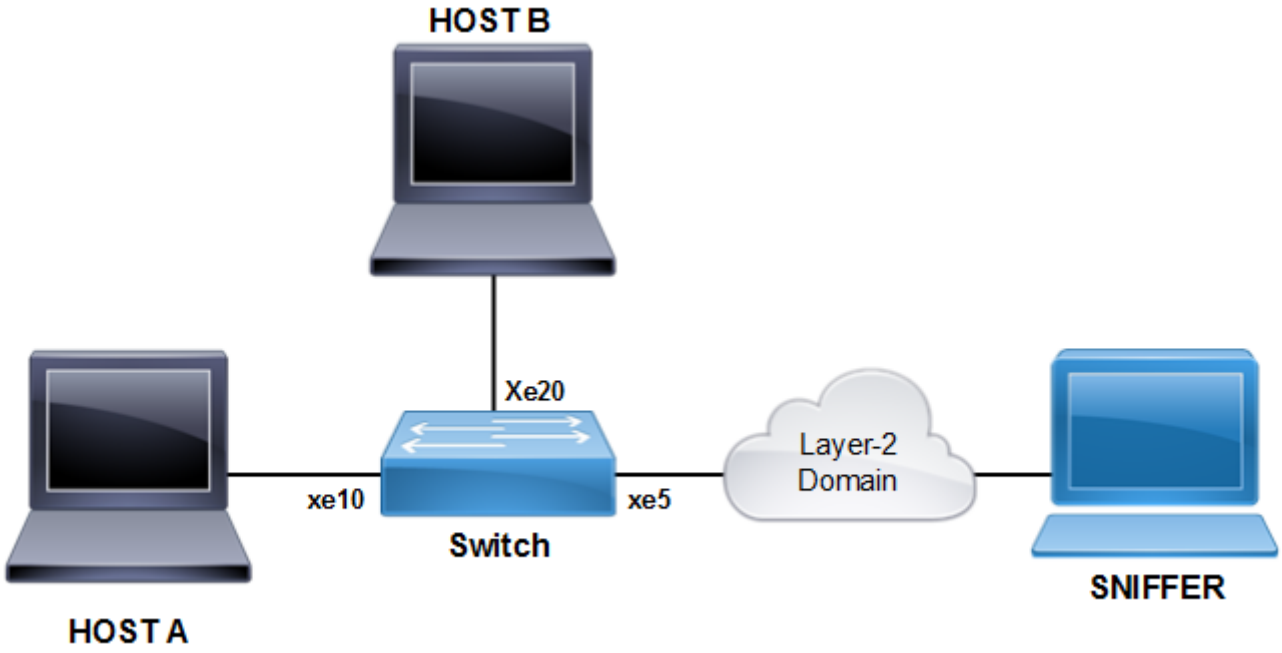


Figure 10-52: RSPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.

(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configurations

```
#show running-config monitor
!
monitor session 1 type remote
 source interface xe10 both
 destination remote vlan 100 reflector-port xe5
 no shut


#show monitor session all
   session 1
---------------
type              : remote
state             : up
source intf       :
    tx            : xe10
    rx            : xe10
    both          : xe10
source VLANs      :
    rx            :
rspan VLAN        : 100
```

```
reflector ports   : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring Configuration

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1 type remote`	Enter monitor session configuration mode.
`(config-monitor)# destination remote vlan 100 reflector-port xe5`	Configure the interface as remote destination port.
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored.
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC.
`(config-monitor)# no shut`	Activate monitor session.
`(config-monitor)#end`	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configuration.

```
#show running-config monitor
!
monitor session 1 type remote
 source vlan 101
```

```
 destination remote vlan 100 reflector-port xe5
 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : remote
state             : up
source intf       :
    tx            :
    rx            :
    both          :
source VLANs      :
    rx            : 101
rspan VLAN        : 100
reflector ports   : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

CHAPTER 11 Port Security Configuration

The Port Security feature allows network administrators to block unauthorized access to the network. Network administrators can configure each port of the switch to allow network access from only secured MACs, so that the switch forwards traffic from only secured MACs.

Users can limit each port's ingress traffic by limiting MAC addresses (source MACs) that are used to send traffic into ports. Port Security enables users to configure the maximum number of secured MACs for each port. Switches learn secured MAC dynamically (learned by switch during traffic inflow) or statically (User configured MACs). Dynamically Learned or statically programmed MAC addresses cannot exceed the maximum number of secured MACs configured for a particular port. Once the switch reaches the maximum limit for secured MACs, traffic from all other MAC addresses are dropped.

The violated MACs are logged in syslog messages. Refer to `cpu queue portsec-drop` using the command `show interface cpu counter queue-stats` for information on the number of violated MACs.

Secured MACs Learned Dynamically

Figure 11-53: Secured MACs learned dynamically

Send Layer 2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1. Because the maximum limit is configured to 3, only 3 secure MAC addresses will be learned by SW1.

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Set the host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2-200 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#switchport port-security`	Enable port security mode dynamic
`(config-if)#switchport port-security maximum 3`	Limit secure MAC to 3 mac addresses.
`(config-if)#exit`	Exit interface mode
`(config)#interface ge2`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk

(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit interface mode
(config)#logging monitor 7	Enable logging level as 7 for debugging

Validation

Validation commands are show port-security, show port-security interface <ifname>, show mac address-table count bridge 1, show bridge, and show mac address-table bridge 1.

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0300.0500    1     100
 1         100                  ge1         0000.0300.055b    1     100
 1         100                  ge1         0000.0300.055c    1     100

SW1#show mac address-table bridge 1

CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
 100          0000.0300.0500   dynamic   ge1       Enable
 100          0000.0300.055b   dynamic   ge1       Enable
 100          0000.0300.055c   dynamic   ge1       Enable
```

Secured MAC Addresses Learned Statically

1. Stop the traffic from IXIA1 and do a `clear mac address-table dynamic bridge 1` on SW1.
2. Verify all dynamic secured MAC addresses are cleared.
3. Configure 3 static secure MAC addresses using the commands below in port security configured interface.
4. Try to add a fourth static secure MAC address.
5. Verify operator log message is displayed, saying "`port security mac limit reached`."

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode

Validation

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3          100           0000.0000.aaaa
                                       100           0000.0000.aaab
                                       100           0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100           0000.0000.aaaa
 100           0000.0000.aaab
 100           0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
```

```
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable

SW1#
```

Remove the port-security configuration method using the two commands below:

`config)#interface ge1`	Enter interface mode
`(config-if)#no switchport port-security`	Set the port-security method to static.

Static Mode

Use the below command to configure the port-security method to static and configure static secure MAC addresses using the commands in static port-security method, below.

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security static`	Set the port-security method as static.
`(config-if)#switchport port-security max 3`	Limit static secure MAC to 3 mac addresses.
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode .

Verify the 3 secure static MAC addresses are added in interface ge1 using show running-config and also verify the port-security method should be static using below show commands.

Validation

```
SW1#show running-config interface ge1
interface ge1
 switchport
bridge-group 1
 switchport mode hybrid
 switchport hybrid allowed vlan all
 switchport port-security static
 switchport port-security maximum 3
 switchport port-security mac-address 0000.0000.aaaa vlanId 100
 switchport port-security mac-address 0000.0000.aaab vlanId 100
```

```
 switchport port-security mac-address 0000.0000.aaac vlanId 100

SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     static              3         100           0000.0000.aaaa
                                      100           0000.0000.aaab
                                      100           0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Static
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+---------------
 100          0000.0000.aaaa
 100          0000.0000.aaab
 100          0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+--------------+---------+---------+-------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable
```

Configure one more static secure MAC address on interface ge1 and try to verify “`port security mac limit reached`” operator log message is displayed.

Start sending Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1, and verify no dynamic secure MAC addresses are being learned using all the validation commands used.

CHAPTER 12 ErrDisable for Link-Flapping Configuration

If a link flaps continuously, the interface goes into ErrDisable state. When a port is the ErrDisable state, it is effectively shut down and no traffic is sent or received on that port. The port can be recovered from the ErrDisable state manually (shutting down the interface) or automatically (setting a timeout value).

Note:

- An interface should change state as up-down to complete one cycle of a link flap.
- Admin shut/no shut will not change interface into errdisable state
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Topology

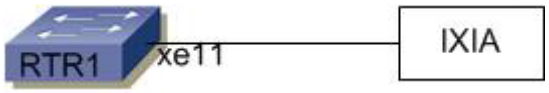


Figure 12-54: ErrDisable

Automatic Recovery

By default, an interface goes into the ErrDisable state when a link flaps 5 times in 10 seconds. An interface is recovered from the ErrDisable state when the configured non-zero errdisable time-out interval value expires.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable ErrDisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 2 time 30`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#errdisable timeout interval 50`	Configure interval to recover from error disable state

Note: Automatic recovery timeout is disabled, if you configure `errdisable timeout interval 0`

Validation

```
#show errdisable details

 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 30 secs
 Link Flaps allowed Max. count : 2
```

```
ErrDisable Cause     Status
---------------      ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
Mac-move-limit       Disabled
```

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

```
#show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          38

#show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
#
```

Note: Interface xe11 went into the ErrDisable state after flapping 2 times in 30 seconds.

Log Message

`Edge1-SiteX#configure terminal`	Enter configure mode.
`Edge1-SiteX(config)#logging level nsm 4`	Enable Operational log to display recovery message

```
2017 Sep 18 11:52:12 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
(config-if)#no shut
(config-if)#2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 11:52:15 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_ERR_DISABLE_DOWN_2]: Interface xe11 moved to
errdisable state due to link-flap
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
```

Note: Interface xe11 recovered from the ErrDisable state after a 50 second time-out.

Manual Recovery

An interface can be recovered manually from the Errdisable state, when configure shutdown followed by no shutdown using CLI. Shutdown will recover the interface from errdisable state and No shutdown will make the interface up state.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable errdisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 3 time 20`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer

```
#show running-config | include errdisable
errdisable cause link-flap
errdisable link-flap-setting max-flaps 3 time 20

#show errdisable details

 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
---------------      ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Disabled
Mac-move-limit       Disabled
```

Note: Interface xe11 went into the ErrDisable state after flapping 3 times in 20 seconds.

```
(config)#do show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          NA
(config)#do show int brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
```

Note: Interface xe11 recovered from the ErrDisable state after entering `shutdown` followed by `no shutdown`.

```
(config)#interface xe11
(config-if)#shutdown
2017 Sep 18 13:02:20 : NSM : WARN : [IFMGR_ERR_DISABLE_UP_4]: Interface xe11 recovered
from link-flap errdisable
(config-if)#no shut
(config-if)#2017 Sep 18 13:02:21 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 13:02:21 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up

config)#do show interface errdisable
(config)#do show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
```

```
(config)#
```

If you configure `no errdisable cause link-flap`, at the global level, it recovers all the interfaces from the ErrDisable state

Errdisable at the Interface Level

If you enable errdisable globally, by default all physical interfaces enable link-flap errdisable. To turn off errdisable for an interface, configure the commands below.

`#configure terminal`	Enter configure mode.
`(config)#interface xe11`	Enter into interface level
`(config-if)#no link-flap errdisable`	Disable link-flap errdisable for interface

Note: If you configure “no link-flap errdisable” in interface level, either it won’t allow the interface move to errdisable state or it will recover interface from errdisable state

Validation

```
#show run int xe11
!
interface xe11
 description *1/2 member of PO3 - Connected to IXIA 6/6*
 channel-group 3 mode active
 no link-flap errdisable
!
```

CHAPTER 13 Private VLAN Configuration

A private VLANs (PVLAN) splits a primary VLAN domain into multiple isolated broadcast sub-domains. PVLAN, also known as port isolation, is a technique where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink.

Topology

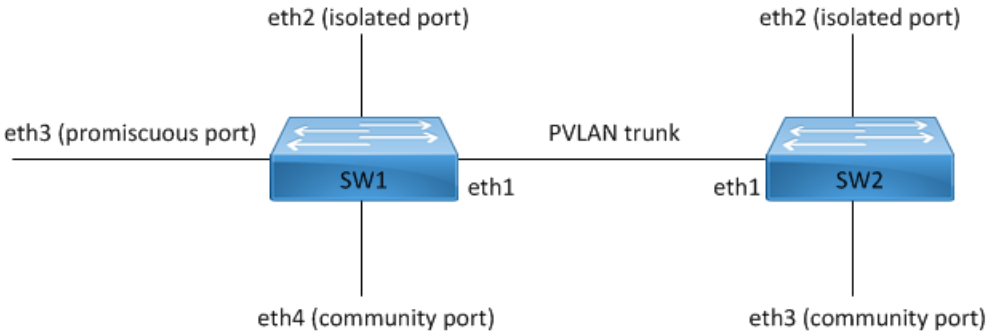


Figure 13-55: PVLAN configuration

Configure PVLAN Trunk and Promiscuous Trunk Port

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW1(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW1(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW1(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW1(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW1(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100

`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface eth3`	Enter interface configuration mode for eth3
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport mode private-vlan promiscuous`	Configure the interface as promiscuous port for private-vlan
`SW1(config-if)#switchport trunk allowed vlan add 100`	Configure VLAN 100 (primary VLAN)
`SW1(config-if)#switchport private-vlan mapping 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#switchport private-vlan mapping 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface eth4`	Enter interface configuration mode for eth4
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#exit`	Exit configuration mode

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW2(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW2(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW2(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW2(config-vlan)#private-vlan 100 primary bridge  1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW2(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW2(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW2(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface eth3`	Enter interface configuration mode for eth3
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan

SW2(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW1(config)#exit	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      eth1,eth2,
     100              20         community      eth1,eth4,
SW1#
SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      eth1,eth2,
     100              20         community      eth1,eth3,
SW2#
```

Configure PVLAN Trunk and Promiscuous Access Port

SW1

SW1#configure terminal	Enter configuration mode
SW1(config)#bridge 1 protocol ieee vlan-bridge	Create bridge
SW1(config)#vlan database	Enter VLAN configuration mode
SW1(config-vlan)#vlan 10 bridge 1 state enable	Create VLAN 10
SW1(config-vlan)#vlan 20 bridge 1 state enable	Create VLAN 20
SW1(config-vlan)#vlan 100 bridge 1 state enable	Create VLAN 100
SW1(config-vlan)#private-vlan 10 isolated bridge 1	Configure VLAN 10 as isolated VLAN
SW1(config-vlan)#private-vlan 20 community bridge 1	Configure VLAN 20 as community VLAN
SW1(config-vlan)#private-vlan 100 primary bridge 1	Configure VLAN 100 as primary VLAN
SW1(config-vlan)#private-vlan 100 association add 10 bridge 1	Associate secondary isolated VLAN 10 with primary VLAN 100
SW1(config-vlan)#private-vlan 100 association add 20 bridge 1	Associate secondary community VLAN 20 with primary VLAN 100
SW1(config-vlan)#exit	Exit VLAN configuration mode
SW1(config)#interface eth1	Enter interface configuration mode for eth1

SW1(config-if)#switchport	Configure switchport
SW1(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW1(config-if)#switchport mode trunk	Set the switching characteristics of this interface as trunk
SW1(config-if)#switchport trunk allowed vlan add 10,20,100	Configure VLAN 10,20,100 (primary, secondary VLANs)
SW1(config-if)#exit	Exit interface mode
SW1(config)#interface eth3	Enter interface configuration mode for eth3
SW1(config-if)#switchport	Configure switchport
SW1(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW1(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW1(config-if)#switchport mode private-vlan promiscuous	Configure the interface as promiscuous port for private-vlan
SW1(config-if)#switchport access vlan 100	Configure VLAN 100 (primary VLAN)
SW1(config-if)#switchport private-vlan mapping 100 add 10	Associate port with primary and secondary VLAN of private-vlan
SW1(config-if)#switchport private-vlan mapping 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW1(config-if)#exit	Exit interface mode
SW1(config)#interface eth4	Enter interface configuration mode for eth4
SW1(config-if)#switchport	Configure switchport
SW1(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW1(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW1(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW1(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW1(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW1(config-if)#exit	Exit interface mode
SW1(config)#interface eth2	Enter interface configuration mode for eth2
SW1(config-if)#switchport	Configure switchport
SW1(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW1(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW1(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW1(config-if)#switchport access vlan 10	Configure VLAN 10 (isolated VLAN)
SW1(config-if)#switchport private-vlan host-association 100 add 10	Associate port with primary and secondary VLAN of private-vlan
SW1(config-if)#exit	Exit interface mode
SW1(config)#exit	Exit configuration mode

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW2(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW2(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW2(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW2(config-vlan)#private-vlan 100 primary bridge  1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW2(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW2(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW2(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface eth3`	Enter interface configuration mode for eth3
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access

SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW1(config)#exit	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      eth1,eth2,
     100              20         community      eth1,eth4,
SW1#
SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      eth1,eth2,
     100              20         community      eth1,eth3,
SW2#
```

CHAPTER 14 Layer 2 Subinterface Configuration

This chapter contains examples of configuring L2 Subinterfaces.

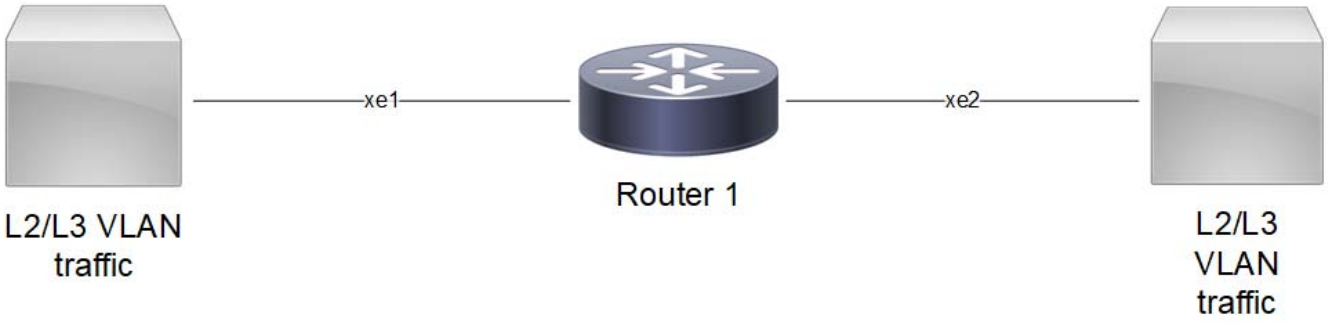
A subinterface is a virtual interface created by dividing a physical interface into multiple logical interfaces. A subinterface on a router uses the parent physical interface for sending and receiving data.

Subinterfaces are used for a variety of purposes. Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN identifiers. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances.

Note: Refer to the release note for features supported by L2 Sub-interface.

Topology

Below figure shows and example of subinterface configuration for one node with cross-connect. In this example, there is one router R1 with 2 connections



The xe1.10 and xe2.10 subinterface is created on R1

Subinterfaces can be created on physical and LAG interfaces in Layer 2 mode (switchport).

Note: Use switchport dot1q ethertype (8100 | 88a8 | 9100 | 9200) command to configure the service-tpid value on parent port of a subinterface. By this the tpid used for service tag for a subinterface may be inherited from the one applied to parent interface.

Note: For any dot1ad subinterface to be functional, switchport dot1q ethertype should be set to desired value as 88a8/9100/9200. Default value is 8100. To verify the ethertype value for the interface use show interface <subinterface> command.

Configure L2 Subinterface with cross-connect

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode
`(config-if)# switchport dot1q ethertype 88a8`	Configure interface with tpid value as 88a8
`(config-if)#interface xe1.10 switchport`	Creates a L2 sub-interface as xe1.10
`(config-if)#encapsulation dot1q 10`	Configure the encapsulation as dot1q matching vlan 10
`(config)#interface xe2`	Enter interface mode
`(config-if)# switchport dot1q ethertype 88a8`	Configure interface with tpid value as 88a8
`(config-if)#interface xe2.10 switchport`	Creates a L2 sub-interface as xe2.10
`(config-if)#encapsulation dot1q 10`	Configure the encapsulation as dot1q matching vlan 10
`(config)# cross-connect CC1`	Create cross-connect with name CC1
`(config-xc)# interface xe1.10`	Attach interface xe1.10
`(config-xc)# interface xe2.10`	Attach interface xe2.10

Creating a Subinterface with Encapsulation

Single encapsulation as dot1q with vlan range

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1q 100-200
```

Single encapsulation as dot1ad with vlan range

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1ad 100-200
```

Double encapsulation as dot1q

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1q 10 inner-dot1q 10
```

Double encapsulation as dot1ad

```
configure terminal (config)#interface xe1.200 switchport
(config-if)# encapsulation dot1ad 20 inner-dot1q 20
```

Encapsulation as default

```
configure terminal (config)#interface xe1.101 switchport
(config-if)# encapsulation default
```

Encapsulation as untagged

```
configure terminal (config)#interface xe1.102 switchport
(config-if)# encapsulation untagged
```

Rewrite with push

```
configure terminal (config)#interface xe1.10 switchport
(config-if)# encapsulation dot1q 10
(config-if)# rewrite push 0x8100 100
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation dot1q 100 inner-dot1q 10
```

```
(config)# cross-connect CC1
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: At interface xe1.10, for incoming traffic "rewrite push" will add vlan as 100 with tpid values 8100.

Note: At interface xe1.10, for outgoing traffic "rewrite push" will pop the vlan.

Rewrite with translate

```
configure terminal (config)# interface xe1
(config-if)# switchport dot1q ethertype 9100
(config-if)#interface xe1.10 switchport
(config-if)# encapsulation dot1ad 200
(config-if)# rewrite translate 0x9100 100
(config-if)#interface xe2
(config-if)# switchport dot1q ethertype 9100
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation dot1ad 100
(config)# cross-connect CC1
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: At interface xe1.10, for incoming traffic "rewrite translate" will update vlan as 100 with tpid values 9100.

Note: At interface xe1.10, for outgoing traffic "rewrite translate" will update vlan as 200 with tpid values 9100.

Rewrite with pop

```
#configure terminal (config)#interface xe1.10 switchport
(config-if)# encapsulation dot1q 100
(config-if)# rewrite pop
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation untagged
(config)# cross-connect CC1
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: At interface xe1.10, for incoming traffic "rewrite pop" will pop the vlan.

Note: At interface xe1.10, for outgoing traffic "rewrite pop" will add vlan as 100 with tpid values 8100.

Note: Push, pop and translate rewrite operations are supported with tpid values 8100/88a8/9100/9200 as symmetric operation.

No subinterfaces

```
#configure terminal (config)#interface xe1
(config-if)# no subinterfaces
```

Note: no Subinterfaces will remove all the Subinterfaces.

Note: Same physical interface will support both L2 and L3 subinterfaces.

L2SI Statistics

Enable below commands to get L2SI statistics

```
#configure terminal (config)# hardware-profile statistics ac-lif enable
```

Note: Reload the node, and then only statistics command will get effective.

Verification commands

Subinterfaces appear as any physical interface in the show running-config or the show ip interface brief output and can be configured as any other interface.

The following examples display subinterface information from various show commands.

show interface brief

```
R1#show interface brief | include xe1
xe1        ETH   --    routed            up      none    10g   --
xe1.10        SUBINTERFACE     up      --     N/A
```

show interface <>

```
R1#show interface xe1.10
Interface xe1.10
  Hardware is SUBINTERFACE  Current HW addr: b86a.97d0.25c5
  Physical:(Not Applicable)  Logical:(not set)
  Port Mode is Switch
  Interface index: 20484106
  Metric 1
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Encapsulation Dot1q (0x8100) Virtual LAN
  Outer Match: Dot1q VLAN 10
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 1g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

show cross-connect

```
R1#show cross-connect
cross-connect status
XC name                       Ep1             Ep2             Status
```

```
-----------------------------+----------------+----------------+-------
CC1                           xe1.10           xe2.10           UP
-----------------------------+----------------+----------------+-------
AC cross-connect summary
Total : 1
Up    : 1
Down  : 0
R1#show running-config interface xe1
!
interface xe1
 switchport dot1q ethertype 0x88a8
!
R1#show run interface xe1.10
!
interface xe1.10 switchport
 encapsulation dot1q 10
 rewrite push 0x8100 10
!
R1#show running-config interface xe1
!
interface xe2
 switchport dot1q ethertype 0x88a8
!
R1#show run interface xe2.10
!
interface xe2.10 switchport
 encapsulation dot1q 10
!
```

show interface xe1.10 counters

```
R1#show interface xe1.10 counters
Interface xe1.10
Rx Packets: 50000
Rx Bytes: 50000000
R1#show interface xe2.10 counters
Interface xe2.10
Tx Packets: 50000
Tx Bytes: 49900000
```

Layer 2 Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Common Commands

This chapter provides a description, the syntax, and examples of common Layer 2 commands.

flowcontrol

Use this command to enable or disable flow control.

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

Use the `no` parameter with this command to disable flow control.

Command Syntax

```
flowcontrol both
flowcontrol send on
flowcontrol send off
flowcontrol receive on
flowcontrol receive off
no flowcontrol
```

Parameters

`both`	Specify flow control mode for sending or receiving.
`send`	Specify flow control mode for sending.
`receive`	Specify the flow control mode for receiving.
`off`	Turn off flow control.
`on`	Turn on flow control.

Default

The flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive off

#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive on
```

```
(config)#interface eth1
(config-if)#no flowcontrol
```

hardware register get

Use this command to get the value of a chip register.

Command Syntax

```
hardware register get ADDR
```

Parameters

ADDR	Register address in 0xhhhh format

Default

By default, hello time is 2 seconds

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#hardware register get 0x3000
```

hardware register set

Use this command to set the value of a chip register.

Command Syntax

```
hardware register set ADDR VALUE
```

Parameters

ADDR	Register address in 0xhhhh format
VALUE	Value

Default

By default, hello time is 2 seconds

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#hardware register set 0x3000 10
```

show flowcontrol

Use this command to display flow control information.

Command Syntax

```
show flowcontrol
show flowcontrol interface IFNAME
```

Parameters

`interface IFNAME`	Specify the name of the interface to be displayed.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show flowcontrol interface` command displaying flow control information:

```
#show flowcontrol interface ge1
Port    Send FlowControl    Receive FlowControl RxPause TxPause

        admin    oper        admin    oper

-----   ------- --------    ------- --------     ------- -------
ge1      on       on           on       on            0       0
#
```

Table 1-84 explains the show command output fields.

Table 1-84: show flow control output

Entry	Description
Port	Interface being checked for flowcontrol.
Send admin	Displays whether the flowcontrol send process is administratively on or off.
FlowControl oper	Displays whether send flowcontrol is on or off on this interface.
Received admin	Displays whether the flowcontrol receive process is administratively on or off.
FlowControl oper	Displays whether receive flowcontrol is on or off on this interface.
RxPause	Number of received pause frames.
TxPause	Number of transmitted pause frames.

show interface capabilities

Use this command to display interface capabilities

Command Syntax

```
show interface (IFNAME|) capabilities
```

Parameters

IFNAME	Displays the name of a specific interface for which status and configuration data is desired.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 capabilities
xe1/1
Speed(FD) : 10MB,100MB,1000MB,10GB,20GB,40GB
Interface : xgmii
Medium : copper
Loopback : none,MAC,PHY
Pause : pause_tx,pause_rx,pause_asymm
Flags : autoneg
Encap : IEEE,HIGIG,HIGIG2
```

Table 1-85 explains the show command output fields.

Table 1-85: show interface capabilities output details

Field	Description
Interface number	The identifying ID number of the interface – eht0, xe1, etc.
Speed (FD)	The Flexible Data-Rates (FD) of the interface
interface	XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of Gigabit Ethernet.
Medium	Members have to have the same medium type configured. This only applies to Ethernet port-channel. Copper, fiber optics, etc.
Loop back	The loop back between the MAC and PHY layers.
Pause	Pause transmit, pause receive, pause asymmetrically.

Table 1-85: show interface capabilities output details

Field	Description
Flags	Interface flags set for Auto-negotiation.
Encap	Encapsulation – IEEE, HIGIG, and HIGIG2 specifications – HIGIG is a proprietary protocol that is implemented by Broadcom. The HIGIG protocol supports various switching functions. The physical signaling across the interface is XAUI, four differential pairs for receive and transmit (SerDes), each operating at 3.125 Gbit/s.

snmp restart mstp

Use this command to restart SNMP in Multiple Spanning Tree Protocol (MSTP).

Command Syntax

```
snmp restart mstp
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart mstp
```

CHAPTER 2 Bridge Commands

This chapter provides a description, syntax, and examples of the bridge commands. It includes the following commands:

bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

Use the no parameter with this command to disable learning.

Note: OcNOS supports only configuration of a single bridge.

Command Syntax

```
bridge <1-32> acquire
no bridge <1-32> acquire
```

Parameter

<1-32>	Bridge group ID.

Default

By default, learning is enabled for all instances.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 acquire
(config)#no bridge 3 acquire
```

bridge address

Use this command to add a static forwarding table entry for the bridge.

Use the no parameter with this command to remove the entry for the bridge

Command Syntax

```
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
bridge <1-32> address XXXX.XXXX.XXXX  (forward|discard) IFNAME vlan <2-4094> svlan
  <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME
no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
  svlan <2-4094>
```

Parameters

<1-32>	Bridge identifier
XXXX.XXXX.XXXX	Media Access Control (MAC) address in HHHH.HHHH.HHHH format.
forward	Forward matching frames.
discard	Discard matching frames.
IFNAME	Interface on which the frame comes out.
vlan	Identity of the VLAN in the range of <2-4094>.
svlan	Identity of the SVLAN in the range of <2-4094>.

Defaul

By default, bridge address is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 address 0000.000a.0021 forward eth0
(config)#no bridge 1 address 0000.000a.0021 forward eth0
```

bridge ageing

Use this command to specify the aging time for a learned MAC address. A learned MAC address persists until this specified time.

Note: The bridge aging time affects the ARP entries which are dependent upon the MAC addresses in hardware. If a MAC address ages out, it causes the corresponding ARP entry to refresh.

Note: On Qumran, the MAC aging time can vary by up to 16%. For example, if the MAC aging time is set to 60 seconds, the aging time can happen anywhere between 50-60 seconds.

Use the `no` form of this command to set the MAC address aging time to its default (300).

Use the `disable` form of this command to turn off MAC address aging completely.

Command Syntax

```
bridge <1-32> ageing-time <10-572>
no bridge <1-32> ageing-time
bridge <1-32> ageing disable
```

Parameters

`<1-32>`	Bridge group ID.
`<10-572>`	Aging time in seconds.
`disable`	Turn off MAC address aging completely.

Default

By default, the aging time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 ageing-time 1000
(config)#no bridge 3 ageing-time
```

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the no parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
bridge <1-32> forward-time <4-30>
no bridge <1-32> forward-time
```

Parameters

<1-32>	Specify the bridge group ID.
<4-30>	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

By default, value is 15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.This value is used by all instances.

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (2 seconds by default).

Use the no parameter to restore the default value of the hello time.

Note: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> hello-time <1-10>
no bridge <1-32> hello-time
```

Parameters

<1-32>	Specify the bridge group ID.
<1-10>	Specify the hello BPDU interval in seconds.

Default

By default, value is 2 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 hello-time 3

(config)#no bridge 3 hello-time
```

bridge mac-priority-override

Use this command to set a MAC priority override.

Use the no parameter with this command to unset a MAC priority override.

Command Syntax

```
bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
  (static|static-priority-override|static-mgmt|static-mgmt-priority-overide)
  priority <0-7>
no bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
```

Parameters

`<1-32>`	Specify the bridge group ID.
`mac-address`	Enter a MAC address in HHHH.HHHH.HHHH format.
`interface`	Interface information
`vlan`	Add the values associated with a single VLAN
`static`	The MAC is a static entry
`static-mgmt`	The MAC is a Static Management
`static-mgmt-priority-overide`	The MAC is a Static Management with priority override
`static-priority-override`	The MAC is a static with priority override
`priority`	priority <0-7> priority value

Default

No default address is specified

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 mac-priority-override mac-address 1111.1111.1111 interface
eth1 vlan 2 static priority 2

(config)#no bridge 1 mac-priority-override mac-address 1111.1111.1111
interface eth1 vlan 2
```

bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances.

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Use the `no` parameter with this command to restore the default value of the maximum age.

Note: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> max-age <6-40>
no bridge <1-32> max-age
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<6-40>`	Specify the maximum time, in seconds, to listen for the root bridge <6-40>.

Default

By default, bridge maximum age is 20 seconds

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 max-age 12

(config)#no bridge 2 max-age
```

bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

Use the no parameter with this command to restore the default value.

Command Syntax

```
bridge <1-32> max-hops <1-40>
no bridge <1-32> max-hops
```

Parameters

<1-32>	Specify the bridge-group ID.
<1-40>	Specify the maximum hops for which the BPDU will be valid <1-40>.

Default

By default, maximum hops in an MST region are 20

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 max-hops 25

#configure terminal
(config)#no bridge 3 max-hops
```

bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root. The priority values can be set only in increments of 4096.

Use the no form of the command to reset it to the default value.

Command Syntax

```
bridge (<1-32> | ) priority <0-61440>
no bridge (<1-32> | )priority
```

Parameters

<1-32>	Specify the bridge group ID.
<0-61440>	Specify the bridge priority in the range of <0-61440>.

Default

By default, priority is 32768 (or hex 0x8000).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 priority 4096

(config)#no bridge 2 priority
```

bridge shutdown

Use this command to disable a bridge.

Use the no parameter to reset the bridge.

Command Syntax

```
bridge shutdown <1-32>
bridge shutdown <1-32> bridge-forward
no bridge shutdown <1-32>
```

Parameters

<1-32>	Specify the bridge group ID.
bridge-forward	Put all ports of the bridge into forwarding state

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge shutdown 4
(config)#no bridge shutdown 4
```

bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the no parameter with this command to restore the default transmit hold-count value.

Command Syntax

```
bridge <1-32> transmit-holdcount <1-10>
no bridge <1-32> transmit-holdcount
```

Parameters

<1-32>	Specify the bridge group ID.
<1-10>	Transmit hold-count value.

Default

By default, transmit hold-count is 6

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 transmit-holdcount 5

(config)#no bridge 1 transmit-holdcount
```

bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

Use the no parameter with this command to disable this command.

Command Syntax

```
bridge-group (<1-32>)
no bridge-group (<1-32>)
```

Parameters

<1-32>	Specify the bridge group ID.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 2

(config)#interface eth1
(config-if)#no bridge-group 2
```

bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

Use the no parameter with this command to restore the default priority value.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

<1-32>	Specify the bridge group ID.
path-cost	Specify the path-cost of a port.
<1-200000000>	Specify the cost to be assigned to the group.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 3 path-cost 123

(config-if)#no bridge-group 3 path-cost
```

bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax

```
bridge-group <1-32> priority <0-240>
no bridge-group <1-32> priority
```

Parameters

<1-32>	Specify the bridge group ID.
<0-240>	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 4 priority 96

(config)#interface eth1
(config-if)#no bridge-group 4 priority
```

clear allowed-ethertype

Use this command to clear statistics for each ethertype per interfaces.

```
clear allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear allowed-ethertype statistics xe54/1

#show allowed-ethertype statistics xe54/1
Interface xe54/1
arp: 0 Packets, 0 Bytes
ipv4: 0 Packets, 0 Bytes
ipv6: 0 Packets, 0 Bytes
dropped: 0 Packets, 0 Bytes
```

clear mac address-table

Use this command to clear the filtering database for the bridge. This command can be issued to do the following:

- clear the filtering database
- clear all filtering database entries configured through CLI (static)
- clear all multicast filtering database entries
- clear all multicast filtering database entries for a given VLAN or interface
- clear all static or multicast database entries based on a mac address

Command Syntax

```
clear mac address-table (dynamic|static|multicast) bridge <1-32>
clear mac address-table (dynamic|static|multicast) (address MACADDR | interface
  IFNAME | vlan VID ) bridge <1-32>
clear mac address-table (dynamic|static|multicast) (address MACADDR | interface
  IFNAME | vlan VID ) (instance INST) bridge <1-32>
clear mac address-table (dynamic|static|multicast) cvlan VID svlan VID bridge <1-
  32>
```

Parameters

`dynamic`	Clears all dynamic entries.
`multicast`	Clears all multicast filtering database entries.
`static`	Clears all entries configured through management.
`address`	Clear the specified MAC Address.
`MACADDR`	When filtering database, entries are cleared based on the MAC address.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`cvlan`	Clears all MAC address for the specified CVLAN. Value range is 1-4094.
`svlan`	Clears all mac address for the specified SVLAN. Value range is 1-4094.
`interface`	Clears all MAC address for the specified interface.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`instance`	Clears MSTP instance ID. Value range is <1-63>.
`vlan`	Clears all MAC address for the specified VLAN. Value range is 1-4094.
`bridge`	Clears the bridge group ID. Value range is 1-32.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to clear all filtering database entries configured through CLI:

```
#clear mac address-table static bridge 1
```

This example shows how to clear multicast filtering database entries:

```
#clear mac address-table multicast bridge 1
```

This example shows how to clear all filtering database entries for a given interface:

```
#clear mac address-table static interface eth0 bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
#clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear static filtering database entries for a given MAC address:

```
#clear mac address-table static address 0202.0202.0202 bridge 1
```

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
#clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

show allowed-ethertype

Use this command to show allowed and denied traffic statistics.

Note: Dropped slow protocol packets provides the count of slow protocol packets among the total dropped count. Total drop count is fetched from hardware and slow protocol packet count is fetched from software. Hence there can be one or two packet difference.

Command Syntax

```
show allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show allowed-ethertype statistics
Interface po1
arp : 0 Packets, 0 Bytes
ipv4 : 511016709 Packets, 184897169366 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 220 Packets, 28160 Bytes
dropped slow protocol pkts : lacp 220, efm 0, others 0
Interface xe47
arp : 0 Packets, 0 Bytes
ipv4 : 169763534 Packets, 61427990740 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
Interface xe48
arp : 0 Packets, 0 Bytes
ipv4 : 0 Packets, 0 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
```

show bridge

Use this command to display the filtering database for the bridge. The filtering database is used by a switch to store the MAC addresses that have been learned and which ports that MAC address was learned on.

Command Syntax

```
show bridge (ieee|rpvst+|mstp|)
```

Parameters

`ieee`	STP bridges.
`rpvst+`	RPVST+ bridges.
`mstp`	MSTP bridges.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   eth1        5254.0029.929c    1     0
 1         2                   eth1        5254.004c.dcc6    1     297
 1         1                   eth1        5254.004c.dcc6    1     291
```

Table 2-86 explains the show command output fields.

Table 2-86: show bridge output fields

Field	Description
Bridge	Bridge identifier.
VLAN, SVLAN, BVLAN	CVLAN, SVLAN, and BVLAN identifiers.
Port	Interface name.
MAC Address	Learned MAC address.
FWD	Whether frames for the MAC addresses are forwarded.
Time-out	How long the learned MAC address persists.

show interface switchport

Use this command to display the characteristics of the interface with the current VLAN.

Command Syntax

```
show interface switchport bridge <1-32>
```

Parameter

`bridge`	Bridge name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
#show interface switchport bridge 2
 Interface name         : eth5
 Switchport mode        : access
 Ingress filter         : disable
 Acceptable frame types : all
 Vid swap               : disable
 Default vlan           : 2
 Configured vlans       :    2
 Interface name         : eth4
 Switchport mode        : access
 Ingress filter         : disable
 Acceptable frame types : all
 Vid swap               : disable
 Default vlan           : 1
 Configured vlans       :    1
```

Table 2-87 explains the show command output fields.

Table 2-87: show interface switchport output fields

Field	Description
Interface name	Display the name of interface.
Switchport mode	Port that used to connect between switches and access port.
Ingress filter	Ingress filtering examines all inbound packets and then permits or denies entry to the network.
Acceptable frame types	Type of acceptable frame in the interface.
VID swap	Displays the status of the VID swap.

Table 2-87: show interface switchport output fields (Continued)

Field	Description
Default vlan	Default value for the VLAN.
Configured vlans	Displays the information on configured VLANs.

show mac address-table count bridge

Use this command to display a count of MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) count bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> | svlan <1-4094>}|)
```

Parameter

`local`	Local dynamic FDB entries
`remote`	Remote dynamic FDB entries
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier
`<1-4094>`	SVLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3
```

Table 2-88 explains the show command output fields.

Table 2-88: show mac address-table count output fields

Field	Description
Dynamic Address Count	Number of dynamic addresses.
Unicast MAC Address Count	Number of unicast addresses.
Multicast MAC Address Count	Number of multicast addresses.
Total MAC Addresses	Total number of addresses.

show mac address-table bridge

Use this command to display MAC entries from the filtering database.

Note: The hardware can learn the MAC address at line rate, but OcNOS will learn the MAC address at a much slower rate. The learning in OcNOS will also depend upon the current load in the system. Under normal conditions OcNOS can learn the mac-address at approximately 3000 MACs per sec.

Command Syntax

```
show mac address-table (local|remote|) bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> | svlan <1-4094>}|)
```

Parameter

`local`	Local dynamic FDB entries
`remote`	Remote dynamic FDB entries
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier
`<1-4094>`	SVLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table bridge 1
 CVLAN  SVLAN  MAC Address       Type      Ports     Port-security
------+------+---------------+---------+---------+-------------
 100   200    1111.2222.1111  static    xe12      Disable
 102   202    1111.2222.1111  static    xe12      Disable
       201    1111.1111.1111  static    xe14      Disable
       202    1111.1111.1111  static    xe14      Disable
       203    1111.1111.1111  static    xe14      Disable
       201    0000.0700.0d00  dynamic   xe14      Disable
       202    0000.0700.0d00  dynamic   xe14      Disable
       203    0000.0700.0d00  dynamic   xe14      Disable
       204    0000.0700.0d00  dynamic   xe14      Disable
       205    0000.0700.0d00  dynamic   xe14      Disable
       206    0000.0700.0d00  dynamic   xe14      Disable
       207    0000.0700.0d00  dynamic   xe14      Disable
       208    0000.0700.0d00  dynamic   xe14      Disable
       209    0000.0700.0d00  dynamic   xe14      Disable
```

```
103   203    0000.0700.0b00  dynamic   xe12      Disable
101   201    0000.0700.0b00  dynamic   xe12      Disable
100   200    0000.0700.0b00  dynamic   xe12      Disable
102   202    0000.0700.0b00   dynamic     xe12        Disable
```

Table 2-89 explains the show command output fields.

Table 2-89: show mac address-table output fields

Field	Description
VLAN	VLAN identifier.
MAC Address	Media Access Control address.
Type	Dynamic, multicast, or static.
Ports	Interface name.

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no switchport
```

Parameters

None

Default

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport
```

switchport allowed ethertype

Use this command to allow a set of ethertype on the access port and deny remaining traffic.

Use the no command to remove ethertype configuration.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|WORD|log}
no switchport allowed ethertype ({arp|ipv4|ipv6|mpls|WORD|log}|)
```

Parameters

`arp`	Ethertype 0x0806.
`ipv4`	Ethertype 0x0800.
`ipv6`	Ethertype 0x086dd.
`mpls`	Ethertype 0x8847.
`WORD`	Any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport allowed ethertype arp ipv4 ipv6 log

(config-if)#no switchport allowed ethertype ipv4
```

CHAPTER 3 Spanning Tree Protocol Commands

This chapter provides a description, syntax, and examples of the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) commands. It includes the following commands:

bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for MSTP (Multiple Spanning Tree Protocol).

If Cisco interoperability is required, all OcNOS devices in the switched LAN must be Cisco-interoperability enabled. When OcNOS inter operates with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN-to-instance mapping is not used to classify regions when interoperating with Cisco.

Command Syntax

```
bridge <1-32> cisco-interoperability (enable | disable)
```

Parameters

`<1-32>`	Specify the bridge group ID
`enable`	Enable Cisco interoperability for MSTP bridge
`disable`	Disable Cisco interoperability for MSTP bridge

Default

By default, cisco interoperability is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To enable Cisco interoperability on a switch for a bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a switch for a particular bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability disable
```

bridge instance

Use this command to add an MST instance to a bridge.

Use the no form of this command to delete an MST instance identifier from a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>)
no bridge (<1-32> | backbone) instance (<1-63>)
```

Parameters

<1-32>	Bridge identifier.
backbone	Backbone bridge.
<1-63>	MST instance identifier.

Default

The bridge instance default is 1.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 4 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3
...
(config-mst)#no bridge 4 instance 3
```

bridge instance priority

Use this command to set the bridge instance priority.

Use the no form of this command to reset the priority to its default.

Command Syntax

```
bridge (<1-32> | backbone) instance <1-63> priority <0-61440>
no bridge (<1-32> | backbone) instance <1-63> priority
```

Parameters

<1-32>	Specify the bridge identifier.
backbone	Specifies the backbone bridge.
<1-63>	Specify the instance identifier.
priority	Specify the bridge priority for the instance. The lower the priority of the bridge, the better the chances is of the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096. The default value is 32768.
<0-61440>	Specify the bridge priority.

Default

By default, bridge instance priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#bridge 4 instance 3 priority 1
```

bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge.The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

Use the no form of this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
no bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
```

Parameters

<1-32>	Bridge identifier.
backbone	Backbone bridge.
<1-63>	MST instance identifier.
VLANID	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list. For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Default

The bridge instance VLAN ID Interfaces default-switch is VLAN100 100 ae0.0 ae1.0 ae2.0.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
```

```
(config-mst)#no bridge 1 instance 1 vlan 10,11
```

bridge multiple-spanning-tree

Use this command to enable MSTP on a bridge.

Use the no form of this command to disable MSTP on the bridge.

Command Syntax

```
bridge <1-32> multiple-spanning-tree enable
no bridge <1-32> multiple-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

`<1-32>`	Specify the bridge-group ID.
`enable`	Enables the spanning tree protocol.
`bridge-forward`	Puts all ports of the specified bridge into forwarding state.
`bridge-block`	Puts all ports of the specified bridge into blocking state.

Default

If the bridge-forward option is entered when using the no parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> multiple-spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 multiple-spanning-tree enable

#configure terminal
(config)#no bridge 2 multiple-spanning-tree enable bridge-forward
```

bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol ieee (vlan-bridge|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`vlan-bridge`	Specify this as a VLAN-aware bridge.

Default

The bridge protocol default value is 2 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 protocol ieee

(config)#bridge 4 protocol ieee vlan-bridge
```

bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter. This command creates an instance of the spanning tree and associates the VLANs specified with that instance.

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability. A bridge created with this command forms its own separate region unless it is added explicitly to a region using the `region name` command.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol mstp (ring|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`ring`	(Optional) Enable rapid ring spanning-tree.

Default

The bridge protocol mstp default value is 50 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol mstp

#configure terminal
(config)#bridge 2 protocol mstp ring
```

bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in Interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol rstp
bridge <1-32> protocol rstp (vlan-bridge|)(ring|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`ring`	(Optional) Add an RSTP bridge for a ring topology.
`vlan-bridge`	(Optional) Adds a VLAN-aware bridge.

Default

By default, bridge protocol rstp is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol rstp

#configure terminal
(config)#bridge 3 protocol rstp vlan-bridge
```

bridge rapid-spanning-tree

Use this command to enable or disable RSTP on a specific bridge. Use the `bridge-forward` option with the `no` form of the command to place all ports on the specified bridge into the forwarding state.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a bridge.

Command Syntax

```
bridge <1-32> rapid-spanning-tree enable
no bridge <1-32> rapid-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enables the spanning tree protocol.
`bridge-forward`	(Optional) Puts all ports of the specified bridge into forwarding state.
`bridge-block`	(Optional) Puts all ports of the specified bridge into blocking state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior puts all bridge ports in the forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> rapid-spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
 configure terminal
(config)#bridge 2 rapid-spanning-tree enable

 configure terminal
(config)#no bridge 2 rapid-spanning-tree enable bridge-forward
```

bridge region

Use this command to create an MST region and specify its name. MST bridges of a region form different spanning trees for different VLANs.

Use the no form of the command to disable the Rapid Spanning Tree protocol on a region.

Command Syntax

```
bridge <1-32> region REGION_NAME
no bridge <1-32> region
```

Parameters

<1-32>	Specify the bridge group ID.
REGION_NAME	Specify the name of the region.

Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 region myRegion

(config)#spanning-tree mst configuration
(config-mst)#no bridge 3 region
```

bridge revision

Use this command to specify the number for configuration information.

Command Syntax

```
bridge <1-32> revision <0-65535>
```

Parameters

<1-32>	Specify the bridge group ID in the range of <1-32>.
<0-65535>	Specify a revision number in the range of <0-65535>.

Default

By default, revision number is 0

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 revision 25
```

bridge spanning-tree

Use this command to enable the Spanning Tree Protocol on a bridge.

Use the no parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax

```
bridge <1-32> spanning-tree enable
no bridge <1-32> spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

<1-32>	Specify the bridge group ID.
enable	Enables the spanning tree protocol on this bridge.
bridge-forward	Puts all ports of the specified bridge into the forwarding state.
bridge-block	Puts all ports of the specified bridge into the blocking state.

Default

If the bridge-forward option is entered when using the no parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 spanning-tree enable

#configure terminal
(config)#no bridge 2 spanning-tree enable bridge-forward
```

bridge spanning-tree errdisable-timeout

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval.

Use the no parameter to disable the error-disable-timeout facility.

Command Syntax

```
bridge <1-32> spanning-tree errdisable-timeout enable
no bridge <1-32> spanning-tree errdisable-timeout enable
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enable the timeout mechanism for the port to be enabled back

Default

By default, the port is enabled after 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree errdisable-timeout enable
```

bridge spanning-tree force-version

Use this command to set the version for the bridge. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-4, for RSTP, the valid range is 0-2. When the force-version is set for a bridge, all ports of the bridge have the same spanning tree version set.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to disable the version for the bridge.

Command Syntax

```
bridge <1-32> spanning-tree force-version <0-4>
no bridge <1-32> spanning-tree force-version
```

Parameters

`<1-32>`	Specify the bridge group ID.
`force-version`	Specify a force version identifier:
`0`	STP
`1`	Not supported
`2`	RSTP
`3`	MSTP

Default

By default, spanning tree force version is 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Set the value to enforce the spanning tree protocol:

```
#configure terminal
(config)#bridge 1 spanning-tree force-version 0

(config)#no bridge 1 spanning-tree force-version
```

bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

If the short parameter is used, the switch uses a value for the default path cost a number in the range 1 through 65,535. If the long parameter is used, the switch uses a value for the default path cost a number in the range 1 through 200,000,000. Use the show spanning-tree to view the administratively configured and current running pathcost method running on a bridge.

Use the no option with this command to return the path cost method to the default setting.

Command Syntax

```
bridge <1-32> spanning-tree pathcost method (short|long)
no bridge <1-32> spanning-tree pathcost method
```

Parameters

`<1-32>`	Specify the bridge group ID.
`method`	Method used to calculate default port path cost.
`long`	Use 16-bit based values for default port path costs.
`short`	Use 32-bit based values for default port path costs.

Default

By default, path cost method for STP is short and for MSTP/RSTP is long.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree pathcost method short

(config)#no bridge 1 spanning-tree pathcost method
```

bridge spanning-tree portfast

Use this command to set the portfast BPDU (Bridge Protocol Data Unit) guard or filter for the bridge.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to disable the BPDU filter for the bridge.

BPDU Filter

All ports that have their BPDU filter set to default take the same value of BPDU filter as that of the bridge. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures that PortFast-enabled ports do not transmit or receive any BPDUs.

BPDU Guard

When the BPDU guard feature is set for a bridge, all portfast-enabled ports of the bridge that have the BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. You can either bring the port back up manually by using the `no shutdown` command, or configure the errdisable-timeout feature to enable the port after the specified time interval.

Command Syntax

```
bridge <1-32> spanning-tree portfast bpdu-guard
bridge <1-32> spanning-tree portfast bpdu-filter
no bridge <1-32> spanning-tree portfast bpdu-guard
no bridge <1-32> spanning-tree portfast bpdu-filter
```

Parameters

`<1-32>`	Specify the bridge group ID.
`bpdu-filter`	Specify to filter the BPDUs on portfast enabled ports.
`bpdu-guard`	Specify to guard the portfast ports against BPDU receive.

Default

By default, portfast for STP is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 spanning-tree portfast bpdu-filter

#configure terminal
(config)#bridge 1 spanning-tree portfast bpdu-guard
```

bridge te-msti

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI).

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti
no bridge (<1-32> | backbone) te-msti
```

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
te-msti	MSTI to be the traffic engineering MSTI instance.

Default

By default, bridge te-msti is disabled

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti

(config-te-msti)#no bridge 2 te-msti
```

bridge te-msti vlan

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI). When an MSTI is shutdown (disabled) each VLAN in the MSTI is set to the forwarding state on all bridge ports which the VLAN as a member of. When and MSTI is enabled (no shutdown), normal MSTP operation is started for the MSTI.

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees. All VLANs that do not want spanning tree topology computation need to be assigned to this te-msti instance.

This command is intended for supporting Traffic Engineering (TE) Ethernet tunnels. All VLANs allocated for traffic engineering should be assigned to one MSTI. That MSTI can in turn shutdown the spanning tree operation so that each VLAN path through the network can be manually provisioned.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti vlan <1-4094>
no bridge (<1-32> | backbone) te-msti vlan <1-4094>
```

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
vlan	Specify a VLAN.
<1-4094>	Specify a VLAN identifier to be associated.

Note: This designated instance is defined in 802.1Qay clause 8.9 to be 0xFFE.

Default

By default, te-msti vlan is vlan1.

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti vlan 10
(config-te-msti)#no bridge 2 te-msti vlan 10
```

bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the no form of this command to remove the interface from the MST instance.

Command Syntax

```
bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
no bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`te-msti`	Traffic engineering MSTI instance.
	For Provider Backbone Bridging (PBB), bridge-group <1-32> refers to the I-component or PB bridge while the <backbone> bridge group refers to the B-component. Usually for a BEB (Backbone Edge Bridge) device, the backbone bridge-group is used for traffic engineering.
	For a PB (Provider Bridge) device used as BCB (Backbone Core Bridge), bridge group <1-32> is used for traffic engineering.

Default

By default, the bridge port remains in the listening and learning states for 15 seconds before transitional to the forwarding state.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 1
(config-if)#bridge-group 1 instance te-msti
```

bridge-group instance path-cost

Use this command to set a path cost for a multiple spanning tree instance.

Before you can give this command, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` form of this command to set the path cost to its default which varies depending on bandwidth.

Command Syntax

```
bridge-group (<1-32> | backbone) instance <1-63> path-cost <1-200000000>
no bridge-group ( <1-32> | backbone) instance <1-63> path-cost
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Specify the backbone bridge.
`<1-63>`	Set the MST instance identifier.
`<1-200000000>`	Path cost for a port (a lower path cost means greater likelihood of becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4 instance 3
(config-if)#bridge-group 4 instance 3 path-cost 1000
```

bridge-group instance priority

Use this command to set the priority of a multiple spanning tree instance.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32>) instance (<1-63>) priority <0-240>
no bridge-group (<1-32>) instance (<1-63>) priority
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`<0-240>`	Port priority. A lower value means greater likelihood of becoming root. Set the port priority in increments of 16.

Default

By default, the port priority is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth2
(config-if)#bridge-group 2
(config-if)#bridge-group 2 instance 4
(config-if)#bridge-group 2 instance 4 priority 64
```

bridge-group path-cost

Use this command to set the cost of a path. Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` parameter with this command to restore the default cost value of the path which varies depending on the bandwidth.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the cost of path for a port.
`<1-200000000>`	Specify the cost of the path (a lower cost means a greater likelihood of the interface becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4
(config-if)#bridge-group 4 path-cost 1000
```

bridge-group priority

Use this command to set the port priority for a bridge group.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32> | backbone) priority <0-240>
no bridge-group (<1-32> | backbone) priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`backbone`	Backbone bridge.
`<0-240>`	Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, port priority for each instance is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 4 priority 80
```

bridge-group spanning-tree

This command is used to enable or disable the spanning-tree on a configured bridge.

Command Syntax

```
bridge-group <1-32> spanning-tree (disable|enable)
```

Parameters

`<1-32>`	Specify the bridge group ID.
`disable`	Disable spanning tree on the interface.
`enable`	Enable spanning tree on the interface.

Default

By default, spanning-tree is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#bridge-group 1 spanning-tree enable
```

clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface. This command begins the port migration as per IEEE 802.1w-2001, Section 17.26. After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

Command Syntax

```
clear spanning-tree detected protocols bridge <1-32>
```

Parameters

<1-32>	Specify the bridge group ID.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree detected protocols bridge 2
```

clear spanning-tree statistics

Use this command to clear all STP BPDU statistics.

Command Syntax

```
clear spanning-tree statistics bridge <1-32>
clear spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <1-4094>)
  bridge <1-32>
clear spanning-tree statistics (interface IFNAME| (instance (<1-63>)| vlan <2-
  4094>)) bridge <1-32>
```

Parameters

<1-32>	Specify the bridge identifier.
IFNAME	Specify the name of the interface on which protocols have to be cleared.
<1-63>	MST instance ID.
<1-4094>	VLAN identifier where spanning tree is located <2-4094>

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree statistics bridge 32
```

customer-spanning-tree customer-edge path-cost

Use this command to set the cost of a path associated with a customer edge port on a customer edge spanning tree.

Use the no form of this command to remove the cost of a path associated with a customer edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge path-cost <1-200000000>
no customer-spanning-tree customer-edge path-cost
```

Parameters

`path-cost`	Specify the path-cost of a port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge path-cost 1000
```

customer-spanning-tree customer-edge priority

Use this command to set the port priority for a customer-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge priority <0-240>
```

Parameters

`priority`	Specify the port priority.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge priority 100
```

customer-spanning-tree forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the no form of this command to restore the default value of 15 seconds.

Command Syntax

```
customer-spanning-tree forward-time <4-30>
no customer-spanning-tree forward-time
```

Parameters

<4-30>	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is set to less than 7 seconds.

Default

By default, priority is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree forward-time 6

(config-if)#no customer-spanning-tree forward-time
```

customer-spanning-tree hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). Avoid a very low value of this parameter as this can lead to excessive traffic on the network; a higher value delays the detection of topology change. This value is used by all instances.

Use the `no` option with this command to restore the default value of the hello-time.

Command Syntax

```
customer-spanning-tree hello-time <1-10>
no customer-spanning-tree hello-time
```

Parameters

`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, level is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree hello-time 3

(config-if)#no customer-spanning-tree hello-time
```

customer-spanning-tree max-age

Use this command to set the max-age for a bridge.

Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age should be greater than twice the value of hello-time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by a root can be propagated to the leaf nodes without exceeding the max-age.

Use the no parameter with this command to restore the default value of max-age.

Command Syntax

```
customer-spanning-tree max-age <6-40>
no customer-spanning-tree max-age
```

Parameters

<6-40>	Specify the maximum time in seconds to listen for the root bridge.

Default

By default, bridge max-age is 20 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree max-age 12

(config-if)#no customer-spanning-tree max-age
```

customer-spanning-tree priority

Use this command to set the bridge priority for the spanning tree on a customer edge port. Using a lower priority indicates a greater likelihood of the bridge becoming root. This command must be used to set the priority of the customer spanning tree running on the customer edge port.

Use the no form of the command to reset it to the default value.

Command Syntax

```
customer-spanning-tree priority <0-61440>
no customer-spanning-tree priority
```

Parameters

<0-61440>	Specify the bridge priority in the range <0-61440>. Priority values can be set only in increments of 4096.

Default

By default, priority is 61440

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree priority 4096

(config-if)#no customer-spanning-tree priority
```

customer-spanning-tree provider-edge path-cost

Use this command to set the cost of a path associated with a provider edge port on a customer edge spanning tree.

Use the no form of this command to remove the cost of a path associated with a provider edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> path-cost <1-200000000>
no customer-spanning-tree provider-edge svlan <1-4094> path-cost
```

Parameters

<1-4094>	Specify the SVLAN identifier of provider edge port.
<1-200000000>	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 path-cost 1000

(config-if)#no customer-spanning-tree provider-edge svlan 2 path-cost
```

customer-spanning-tree provider-edge priority

Use this command to set the port priority for a provider-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> priority <0-240>
```

Parameters

`<1-4094>`	Specify the SVLAN identifier of provider edge port.
`<0-240>`	Specify the port priority (a lower priority means greater likelihood of the interface becoming root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 priority 0
```

customer-spanning-tree transmit-holdcount

Use this command to set the transmit-holdcount for a bridge.

Use the no parameter with this command to restore the default value of `transmit-holdcount`.

Command Syntax

```
customer-spanning-tree transmit-holdcount <1-10>
no customer-spanning-tree transmit-holdcount
```

Parameters

`<1-10>`	Specify the maximum number that can be transmitted per second.

Default

By default, bridge transmit hold count is 6

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree transmit-holdcount 3

(config-if)#no customer-spanning-tree transmit-holdcount
```

debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

Note: This command enables MSTP, RSTP, and STP debugging.

Use the no parameter with this command to turn off debugging.

Command Syntax

```
debug mstp all
debug mstp cli
debug mstp packet rx
debug mstp packet tx
debug mstp protocol
debug mstp protocol detail
debug mstp timer
debug mstp timer detail
no debug mstp all
no debug mstp cli
no debug mstp packet rx
no debug mstp packet tx
no debug mstp protocol
no debug mstp protocol detail
no debug mstp timer
no debug mstp timer detail
```

Parameters

`all`	Echoes all spanning-tree debugging levels to the console.
`cli`	Echoes spanning-tree commands to the console.
`packet`	Echoes spanning-tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`detail`	Detailed output.
`timer`	Echoes timer start to the console.
`detail`	Detailed output.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug mstp all
(config)#debug mstp cli
(config)#debug mstp packet rx
(config)#debug mstp protocol detail
(config)#debug mstp timer
```

show debugging mstp

Use this command to display the status of debugging of the MSTP system.

Command Syntax

```
show debugging mstp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging mstp
MSTP debugging status:
MSTP debugging status:
 MSTP timer debugging is on
 MSTP protocol debugging is on
 MSTP detailed protocol debugging is on
 MSTP cli echo debugging is on
 MSTP transmitting packet debugging is on
 MSTP receiving packet debugging is on
#
```

show spanning-tree

Use this command to show the state of the spanning tree for all STP or RSTP bridge-groups, including named interface and VLANs.

Command Syntax

```
show spanning-tree
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst interface IFNAME
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
show spanning-tree vlan range-index
```

Parameters

`interface`	Display interface information
`mst`	Display MST information
`statistics`	Display statistics of the BPDUs
`vlan range-index`	Display a VLAN range-index value
`config`	Display configuration information
`detail`	Display detailed information
`instance`	Display instance information
`<1-63>`	Specify the instance identifier
`te-msti`	Display Traffic Engineering MSTI instance
`<1-32>`	Specify the bridge identifier
`IFNAME`	Display the interface name
`<2-4094>`	Specify a VLAN identifier, associated with the instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying spanning tree information.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
%eth2: Designated Path Cost 0
%eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth2: Designated Port Id 8005 - Priority 128 -
%eth2: Root 80000002b328530a
%eth2: Designated Bridge 80000002b328530a
%eth2: Message Age 0 - Max Age 20
%eth2: Hello Time 2 - Forward Delay 15
%eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth2: forward-transitions 4
%eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%eth2: No portfast configured - Current portfast off
%eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth2: no root guard configured- Current root guard off
%eth2: Configured Link Type point-to-point - Current point-to-point
%eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
%eth1: Designated Path Cost 0
%eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth1: Designated Port Id 8004 - Priority 128 -
%eth1: Root 80000002b328530a
%eth1: Designated Bridge 80000002b328530a
%eth1: Message Age 0 - Max Age 20
%eth1: Hello Time 2 - Forward Delay 15
%eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth1: forward-transitions 4
%eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%eth1: No portfast configured - Current portfast off
%eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth1: no root guard configured- Current root guard off
%eth1: Configured Link Type point-to-point - Current point-to-point
%
%
```

The following is a sample output of this command displaying the state of the spanning tree for interface eth1.

```
#show spanning-tree interface eth1
```

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
```

Table 3-90 Explains the show command output fields.

Table 3-90: show spanning-tree interface output fields

Field	Description
Bridge up	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Root Path Cost	Root cost for the interface.
Root Port	Interface that is the current elected root port for this bridge.
Bridge Priority	Used for the common instance.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Port Id	Logical interface identifier configured to participate in the MSTP instance.
Role Designated	Designated role for the packets in the interface.
State Forwarding	State of the forwarding packets in the interface.
Designated Path Cost	Designated cost for the interface.

Field	Description
Configured Path Cost	Configured cost for the interface.
Designated Port Id	Port ID of the designated port for the LAN segment this interface is attached to.
Priority	Specify the port priority.
Message Age	Number of seconds elapsed since the most recent BPDU was received.
Forward Timer	The forward delay timer is the time interval that is spent in the listening and learning state.
Msg Age Timer	The message age contains the length of time that has passed since the root bridge initially originated the BPDU.
Received RSTP	Number of times the received the RSTP.
Send RSTP	Number of times transmitted the RSTP.

show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

Command Syntax

```
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree mst interface IFNAME
```

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`interface`	Display interface information.
`instance`	Display instance information.
`<1-63>`	Specify the instance identifier.
`te-msti`	Traffic Engineering MSTI instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec%
% Instance VLAN
% 0:        1
% 2:        3-4
```

Table 3-91 Explains the show command output fields.

Table 3-91: show spanning-tree mst output fields

Field	Description
Bridge up	A network bridge is networking process that creates a single aggregate network from multiple communication networks or network segments.
CIST Root Path Cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
CIST Root Port	Interface that is the current elected CIST root port for this bridge.
CIST Bridge	A CIST bridge is networking process that creates a single aggregate network from multiple communication networks.
Priority	Specify the port priority.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Max-hops	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.

show spanning-tree statistics

Use this command to display detailed BPDU statistics for a spanning tree instance.

Command Syntax

```
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
```

Parameters

<1-32>	Bridge identifier.
<1-63>	MST instance identifier.
IFNAME	Displays the interface name.
<2-4094>	Specify a VLAN identifier, associated with the instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, bridge-group 1 is configured for IEEE on the eth2 interface.

```
#show spanning-tree statistics interface eth2 bridge 1

% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Spanning Tree Protocol
% Current Port State                : Learning
% Port ID                           : 8004
% Port Number                       : 4
% Path Cost                         : 200000
% Message Age                       : 0
% Designated Root                   : 00:02:b3:d5:91:ec
% Designated Cost                   : 0
% Designated Bridge                 : 00:02:b3:d5:91:ec
% Designated Port Id                : 8005
% Top Change Ack                    : FALSE
% Configure Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Configure Bpdu's xmitted              : 0
% Configure Bpdu's received             : 22
% TCN Bpdu's xmitted                 : 0
```

```
% TCN Bpdu's received                : 8
% Forward Trans Count                : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured               : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 1
% Forward Delay Timer                : ACTIVE
% Forward Delay Timer Value          : 1
% Message Age Timer                  : ACTIVE
% Message Age Timer Value            : 19
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 14
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 15
% Next State                         : Blocked
% Topology Change Time               : 0


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 00:02:b3:d5:98:3f
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 0
% Last Topology Change Occurred       : Wed Dec 31 16:00:00 1969
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 0
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Table 3-92 Explains the show command output fields.

Table 3-92: show spanning-tree statistics output fields

Field	Description
BPDU Related Parameters	Details of the BPDU related parameters.
PORT Based Information & Statistics	Information of the port and interface for which the statistics are being displayed.

Field	Description
STATUS of Port Timers	Status of the port timers.
Other Port-Specific Info	Specific information about the port.
Other Bridge information & Statistics	Information about bridge and statistics being displayed.

spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the no parameter with this command to disable this feature.

Command Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default

By default, spanning-tree autoedge is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree autoedge
```

spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Note: This command is an alias to the `spanning-tree portfast` command. Both commands can be used interchangeably.

Command Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default

By default, spanning-tree edgeport is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree edgeport
```

spanning-tree guard

Use this command to enable the root guard feature for the port. This feature disables reception of superior BPDUs.

The root guard feature makes sure that the port on which it is enabled is a designated port. If the root guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Use the `no` parameter with this command to disable the root guard feature for the port.

Command Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Parameters

`root`	Set to disable reception of superior BPDUs

Default

By default, spanning-tree guard root is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree guard root
```

spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the no parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax

```
spanning-tree instance <1-63> restricted-role
no spanning-tree instance <1-63> restricted-role
```

Parameters

<1-63>	Specify the instance ID range.

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-role
```

spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Command Syntax

```
spanning-tree instance <1-63> restricted-tcn
no spanning-tree instance <1-63> restricted
```

Parameters

<1-63>	Specify the instance ID range.

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-tcn
```

spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

RSTP has a backward-compatible STP mode, `spanning-tree link-type shared`. An alternative is the `spanning-tree force-version 0`.

Use the no parameter with this command to disable rapid transition.

Command Syntax

```
spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared
no spanning-tree link-type
```

Parameters

`auto`	Sets to either point-to-point or shared based on duplex state.
`point-to-point`	Enables rapid transition.
`shared`	Disables rapid transition.

Default

By default, spanning-tree link-type is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree link-type point-to-point

(config-if)#no spanning-tree link-type
```

spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

Command Syntax

```
spanning-tree mst configuration
```

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#
```

spanning-tree bpdu-filter

Use this command to set the BPDU filter value for individual ports. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge level BPDU filter configuration takes effect for the port.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to revert the port BPDU filter value to default.

Command Syntax

```
spanning-tree bpdu-filter (enable|disable|default)
no spanning-tree bpdu-filter
```

Parameters

`default`	Sets the bpdu-filter to the default level.
`disable`	Disables the BPDU-filter.
`enable`	Enables the BPDU-filter.

Default

By default, spanning-tree bpdu-filter is default option

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-filter enable

(config-if)#no spanning-tree bpdu-filter
```

spanning-tree bpdu-guard

Use this command to enable or disable the BPDU Guard feature on a port.

This command supersedes the bridge level configuration for the BPDU Guard feature. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge-level BPDU Guard configuration takes effect.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

Command Syntax

```
spanning-tree bpdu-guard (enable|disable|default)
no spanning-tree bpdu-guard
```

Parameters

`default`	Sets the BPDU-guard to the default level.
`disable`	Disables the BPDU-guard.
`enable`	Enables the BPDU-guard.

Default

By default, spanning-tree bpdu-guard is default

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-guard enable

(config-if)#no spanning-tree bpdu-guard
```

spanning-tree restricted-domain-role

Use this command to set the restricted-domain-role value of the port to TRUE.

Use the no parameter with this command to set the restricted-domain-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-domain-role
no spanning-tree restricted-domain-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-domain-role
```

spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the no parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the no parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Parameters

None

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-tcn
```

spanning-tree te-msti configuration

This command is used to put the terminal into the `te-msti` configuration mode.

After creating a bridge instance and adding VLAN to that bridge instance, use this command to enter `te-msti` configuration mode.

Command Syntax

```
spanning-tree te-msti configuration
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Use the no form of this command to disable storm control.

Note: Minimum granularity for storm-control is 64kbps.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
  (kbps|mbps|gbps))
no storm-control (broadcast|multicast|dlf)
```

Parameters

`broadcast`	Broadcast rate limiting.
`multicast`	Multicast rate limiting.
`dlf`	Destination lookup failure limiting.
`level`	Sets the percentage of the threshold.
`LEVEL`	The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.
`<0-1000000000>`	Sets absolute threshold value <0-1000000000>
`kbps`	specifies the units of Kilobits per second.
`mbps`	specifies the units of Megabits per second.
`gbps`	specifies the units of Gigabits per second.

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#storm-control broadcast level 30

(config)#interface eth0
(config-if)#storm-control multicast level 30

(config)#interface eth0
```

```
(config-if)#storm-control multicast 300 mbps

(config)#interface eth0
(config-if)#no storm-control multicast
```

CHAPTER 4 Link Aggregation Commands

This chapter describes link aggregation commands.

channel-group mode

Use this command to add an interface to an existing link aggregation group.

After you execute this command, the interface loses its properties and takes the properties of the aggregated interface.

Use the no parameter with this command to remove an interface from a dynamic link aggregation group. When you remove an interface from a LAG, the interface acquires the default interface properties.

Command Syntax

```
channel-group <1-65535> mode (active|passive)
channel-group <1-16383> mode (active|passive)
no channel-group
```

Parameters

`<1-65535>`	Specify a channel group number (without DRNI).
`<1-16383>`	Specify a channel group number (with DRNI).
`mode`	Specify a channel mode.
`active`	Enable LACP negotiation.
`passive`	Disable LACP negotiation.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#exit

#sh run in po1
!
interface po1
 switchport
```

The is an example of `no channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
```

```
!
#sh run in po1
!
interface po1
 switchport

!
```

clear lacp

Use this command to clear the counters of all LACP aggregators or a given LACP aggregator.

Command Syntax

```
clear lacp <1-65535> counters
clear lacp counters
```

Parameters

<1-65535>	Clears a channel-group number.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear lacp 2 counters
```

debug lacp

Use this command to enable LACP debugging.

Use the no parameter with this command to disable debugging.

Command Syntax

```
debug lacp (event|cli|timer|packet|sync|ha|all|rx|tx)
no debug lacp (event|cli|timer|packet|sync|ha|allrx|tx)
undebug all
```

Parameters

`all`	Enables all LACP debugging.
`cli`	Echo commands to console.
`event`	Sets the debug options for LACP events.
`ha`	Echo High availability events to console.
`packet`	Sets the debug option for LACP packets.
`sync`	Echo synchronization to console.
`timer`	Echo timer expiry to console.
`rx`	Echo receiving of lacpdus to console.
`tx`	Echo transmission of lacpdus to console.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug lacp all
```

interface po

Use this command to create a dummy dynamic link aggregate interface (by default an L3 LAG interface).

Use the no form of this command to remove a dynamic link aggregate group and also it remove the properties of the po from all member ports.

Note: Switchport/routed mode needs to be set for the PO before adding member ports to it.

Command Syntax

```
interface po<1-16383>
no interface po<1-16383>
```

Parameters

<1-16383>	Channel group number.

Default

By default, interface po is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#switchport
(config-if)#exit
```

interface sa

Use this command to create a dummy static link aggregate interface (by default an L3 LAG interface) and to add an interface to an existing static link aggregation group.

Use the no form of this command to remove a static link aggregate group and also remove the properties of the po from all member ports.

Command Syntax

```
interface sa<1-16383>
no interface sa<1-16383>
```

Parameters

<1-16383>	Channel group number.

Default

By default, interface sa is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#switchport
(config-if)#exit
```

lacp destination-mac

Use this command to set the address type to use for sending LACPDUs (Link Aggregation Control Protocol Data Units).

Note: The interface must be an aggregation port.

Use the no form of this command to set the address type to its default (multicast group address).

Command Syntax

```
lacp destination-mac  (customer-bridge-group-address | multicast-group-address |
  non-tmpr-group-address)
no lacp destination-mac
```

Parameters

`customer-bridge-group-address`

Customer bridge group address

`multicast-group-address`

Multicast group address (default)

`non-TPMR-group-address`

Non-Two-Port Media Access Control Relay (TPMR) group address

Default

By default, lacp destination-mac is multicast-group-address

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface eth1
(config-if)#lacp destination-mac customer-bridge-group-address
```

lacp discard wrong conversation

Use this command to enable or disable discarding frames with an incorrect port conversation identifier.

Note: The interface must be a dynamic port-channel.

Command Syntax

```
lacp discard wrong conversation (disable|enable)
```

Parameters

`disable`	Do not discard frames with an incorrect port conversation identifier
`enable`	Discard frames with an incorrect port conversation identifier

Default

By default, lacp discard wrong conversation is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface po1
(config-if)#lacp discard wrong conversation enable
```

lacp force-up

Use this command to make a port immediately begin forwarding packets and not wait for an LACPDU. After you execute this command, the member port is forcefully up even if LACP is not in sync (only if no other member in the aggregator is in sync).

If a force-up port stops receiving LACPDUs, the port ignores the time-out and remains in operation.

This command can be configured on one member interface of a port channel.

Note: This command can only be given after executing the channel-group mode command on an interface. Force-up mode is not supported for LACP passive mode.

Note: For MC-LAG, only configure a force-up port on either on the master node or the slave node to prevent traffic drops/loops.

Use the no form of this command to disable force-up mode.

Command Syntax:

```
lacp force-up
no lacp force-up
```

Parameters

None

Default

By default, LACP force-up mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#lacp force-up
(config-if)#exit
```

lacp port-priority

Use this command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the no parameter with this command to set the priority of port to the default value (32768).

Command Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameters

<1-65535>	Specify the LACP port priority.

Default

By default, lacp port priority is 32768

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lacp port-priority 34
```

lacp system-priority

Use this command to set the LACP system priority. This priority determines the system responsible for resolving conflicts in the choice of aggregation groups.

Note: A lower numerical value has a higher priority.

Use the no parameter with this command to set the system priority to its default value (32768).

Command Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameters

<1-65535>	System priority.

Default

By default, system priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lacp system-priority 6700
```

lacp timeout

Use this command to set either a short or long timeout value on a port. The timeout value is the number of seconds before invalidating a received LACP data unit (DU).

Command Syntax

```
lacp timeout (short|long)
```

Parameters

`short`	LACP short timeout. 3 seconds.
`long`	LACP long timeout. 90 seconds.

Default

By default, lacp timeout is long.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sets the LACP short timeout on a port.

```
#configure terminal
(config)#interface eth0
(config-if)#lacp timeout short

#configure terminal
(config)#interface eth0
(config-if)#lacp timeout long
```

port-channel min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG interface.

When a the minimum number of links are configured for a LAG, if the active links for that interface become less than the configured value, then the whole LAG is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the no form of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Note: The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

<2-32>	Minimum number of links

Default

By default, port channel min-link is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

show debugging lacp

Use this command to display the status of the debugging of the LACP system.

Command Syntax

```
show debugging lacp
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging lacp

LACP debugging status:
LACP timer debugging is on
```

show etherchannel

Use this command to display information about link aggregation groups.

Command Syntax

```
show etherchannel
show etherchannel <1-65535>
```

With MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Without MLAG:

```
show etherchannel (<1-65535>|) detail
show etherchannel (<1-65535>|) load-balance
show etherchannel (<1-65535>|) summary
```

Parameters

`<1-65535>`	Specify channel-group number.
`<1-16383>`	Specify channel-group number.
`detail`	Specify detailed etherchannel information.
`load-balance`	Specify load balancing.
`summary`	Specify Etherchannel summary information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show etherchannel summary
% Aggregator po1 185
% Aggregator Type: Layer3
% Admin Key: 0001 - Oper Key 0001
%   Link: eth3 (5) sync: 0
-------------------------------------
% Aggregator po4 186
% Admin Key: 0004 - Oper Key 0004
%   Link: eth2 (4) sync: 0
-------------------------------------
% Aggregator po5 187
% Admin Key: 0005 - Oper Key 0005
%   Link: eth1 (3) sync: 0
```

```
#show etherchannel detail
% Aggregator po1 185
% Aggregator Type: Layer3
%  Mac address: 08:00:27:36:f5:7d
%  Admin Key: 0001 - Oper Key 0001
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0001
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth3 (5) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po4 186
%  Mac address: 08:00:27:76:0c:57
%  Admin Key: 0004 - Oper Key 0004
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0004
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth2 (4) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po5 187
%  Mac address: 08:00:27:2f:d5:ae
%  Admin Key: 0005 - Oper Key 0005
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0005
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth1 (3) sync: 0
%  Collector max delay: 5
```

Table 4-93 explains the show command output fields.

Table 4-93: show etherchannel detail output

Field	Description
Aggregator	Link aggregators name and ID number.
Mac address	Unique MAC address for link identification.
Admin Key	LACP administrative key – automatically configured value on each port configured to use LACP.
Oper Key	LACP operator key on Partner – automatically configured value on each port configured to use LACP.
Actor LAG ID	LAG ID consisting of MAC address plus aggregator ID number for this Actor.
Receive link count	The number of link received from the peer LAG.
Transmit link count	The number of links contained transmitted to the peer LAG.
Individual	The individual physical network interfaces or ports contained in the LAG.
Ready	The number of links in the active state on this Actor.
Partner LAG ID	Partner LAG ID consisting of MAC address plus aggregator ID number.

Table 4-93: show etherchannel detail output (Continued)

Field	Description
Link	Interface and ID number of the link.
sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.
Collector max delay	Maximum period of wait time between sending of two subsequent Ethernet frames on a link.

show lacp sys-id

Use this command to display the LACP system identifier and priority.

Command Syntax

```
show lacp sys-id
```

Parameters

`sys-id`	Display LACP system ID and priority

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp sys-id
% System 8000,00-0e-0c-83-37-27
```

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

Command Syntax

```
show lacp-counte
show lacp-counter <1-65535>
```

Parameters

<1-65535>	Channel-group number

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp-counter 555

Port      LACPDUs         Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
```

show port etherchannel

Use this command to display details about a PO and its members' interfaces or to display details of a single member interface of a PO.

Command Syntax

```
show port etherchannel IFNAME
```

Parameters

IFNAME	Interface name

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show port etherchannel ce29/1
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
  Receive machine state       : Current
  Mux machine state           : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority         : 0x8000 (32768)
  Admin key                   : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key          : (2)
  Actor Oper state            : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state           : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port           : 10009
  Partner link info           : admin port 0
  Partner admin LAG ID        : 0x0000-00:00:00:00:0000
  Partner system priority     : admin:0x0000 - oper:0x8000
  Partner port priority       : admin:0x0000 - oper:0x8000
  Partner oper state          : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state         : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0


#show port etherchannel po2
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
```

```
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10009
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0

LACP link info             : ce30/1 - 10005
Periodic Transmission
machine state              : Slow periodic
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10013
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

Note: Most of the output of this command is duplicated in the show etherchannel command (see also the 802.3ad specificiation). The output of the `show port etherchannel` command is primarily a list of state machine values. An explanation of the state machine bits follows. See Figure 4-56.

Table 4-94 explains the show command output fields.

Table 4-94: show port etherchannel detailed output

Entry	Description
Actor/Partner state	The Actor's and Partner's state variables, encoded as individual bits within a single octet.
ACT	LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP as a 0.

Table 4-94: show port etherchannel detailed output (Continued)

Entry	Description
TIM	LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout as a 0.
AGG	Aggregability is encoded in bit 2. Aggregatable is encoded as a 1; Individual is encoded as a 0.
SYN	Synchronization is encoded in bit 3. In_Sync is encoded as a 1; Out_Of_Sync is encoded as a 0.
COL	Collecting is encoded in bit 4. True is encoded as a 1; False is encoded as a 0.
DIS	Distributing is encoded in bit 5. True is encoded as a 1; False is encoded as a 0.
DEF	Defaulted is encoded in bit 6.
EXP	Defaulted is encoded in bit 7.

Bits 7 and 8 are reserved; these are ignored on receipt and transmitted as zero. However, the received value of these bits is recorded on receipt to accurately reflect the actor's view of the partner's state in outgoing PDUs.

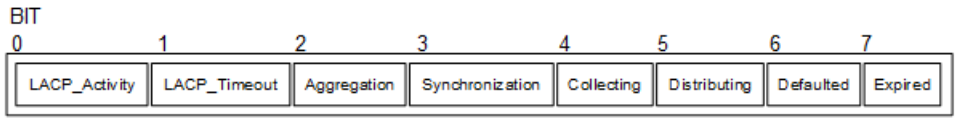


Figure 4-56: Diagram of state machine octet

show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax

```
show static-channel-group  (<1-12>|)
```

Parameters

<1-12>	Specify channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example of the output of this command:

```
#show  static-channel-group 1
% Static Aggregator: sa1
% Member:
   eth1
```

show static-channel load-balance

Use this command to display information about static channel groups.

Command Syntax

```
show static-channel (<1-12>|) load-balance
```

Parameters

<1-12>	Specify static-channel-group number.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS Version 1.0.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Flow based division
```

snmp restart lacp

Use this command to restart SNMP in LACP.

Command Syntax

```
snmp restart lacp
```

Parameters

None

Default

By default, snmp restart lacp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lacp
```

static-channel-group

Use this command to create a static link aggregation group or to add an interface to an existing link aggregation group.

Use the `no` form of this command to remove an interface from a static link aggregation group without removing the static link aggregation group itself.

Command Syntax

```
static-channel-group <1-12>
no static-channel-group
```

Parameter

`<1-12>`	Channel group number.

Default

By default, static channel group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#static-channel-group 1
(config-if)#exit

#sh run in sa1
!
interface sa1
 switchport
```

This is an example of `no static-channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no static-channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
!
#sh run in sa1
!
interface sa1
 switchport
```

!

CHAPTER 5 Multi-chassis Link Aggregation Commands

This chapter describes the Multi-Chassis Link Aggregation commands.

Multi-Chassis Link Aggregation is also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect (DRNI). In this document, it is called MC-LAG.

clear mcec statistics

Use this command to clear the statistics related to hello and information PDUs in the MCEC domain.

Command Syntax

```
clear mcec statistics
```

Parameters

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 4.0.

Examples

```
#clear mcec statistics
```

domain-address

Use this command to configure domain address, which helps to identify the mcec domain.

Use the no form of this command to remove the domain address.

Command Syntax

```
domain-address <domain-id>
no domain-address
```

Parameters

```
domain-id  domain address in HHHH.HHHH.HHHH format
```

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-address 1111.2222.3333
```

debug mcec

Use this command to view debugging logs for MLAG.

Use the no form of this command to remove debugging logs for MLAG.

Command Syntax

```
debug mcec (timer|event|hello|info|cli|mac-sync|all)
no debug mcec (timer|event|hello|info|cli|mac-sync|all)
```

Parameters

`all`	ALL
`cli`	CLI
`event`	Event
`hello`	Hello
`info`	Info
`mac-sync`	Mac Sync
`timer`	Timer

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug mcec all
#no debug mcec all
```

domain hello timeout

Use this command to specify the domain hello-timeout value.

Command Syntax

```
domain-hello-timeout (long|short)
```

Parameters

`long`	Long Timeout
`short`	Short Timeout

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-hello-timeout long
```

domain priority

Use this command to specify the priority value associated with mcec domain.

Use the no form of this command to remove the priority value associated with mcec domain.

Command Syntax

```
domain-priority <1-65535>
no domain-priority
```

Parameters

<1-65535>	Priority Value

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-priority 2
```

domain-system-number

Use this command to configure domain system number, which uniquely identifies domain system in mcec domain.

Use the no form of this command to configure domain system number.

Command Syntax

```
domain-systm-number <1-2>
no domain-systm-number
```

Parameters

<1-2>	Domain System Number

Command Mode

MLAC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-system-number 2
```

intra-domain-link

Use this command to map an interface as intra domain link that connects the domain system with its neighbor in a mcec domain.

Use the no form of this command to unmap the interface configured as intra domain link that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-link <IFNAME>
no intra-domain-link
```

Parameters

IFNAME	Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-link eth2
```

mcec domain configuration

Use this command to enter MCEC Domain configuration mode to configure mcec domain information.

Command Syntax

```
mcec domain configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#
```

mlag

Use this command to map a port-channel to mlag instance.

Note: The interface must be a dynamic port channel.

Note: All MLAG nodes must use the same MAC table size.

Use the no form of this command to un-map the port channel from mlag instance.

Command Syntax

```
mlag <1-256>
no mlag
```

Parameters

<1-256>	MC-LAG identifier

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface po1
(config-if)#mlag 1
```

mode

Use this command to set the MC-LAG mode.

Use the no form of this command to turn off this feature.

Command Syntax

```
mode (active-standby)
no mode (active-standby)
```

Parameters

`active-standby` The interface is ready for transition to the active state if a failure occurs in the other node

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS-SP version 4.0.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#mode active-standby
```

show mlag detail

Use this command to display details about MC-LAG configuration and status.

Command Syntax

```
show mlag <1-256> detail
```

Parameters

<1-256>	MLAG group number

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mlag 1 detail

MLAG-1
Mapped Aggregator : po1
Admin Key : 32769
Oper Key: 16385
Physical properties Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync: IN_SYNC
```

Table 5-95 Shows the output details.

Table 5-95: Show mlag output details

Entry	Description
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.

Table 5-95: Show mlag output details

Entry	Description
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mlag domain

Use this command to display MC-LAG configuration and status.

Command Syntax

```
show mlag domain <details|summary>
```

Parameters

details	details
summary	summary

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number : 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49
Domain Adjacency: UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
Mapped Aggregator: po1
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Total Bandwidth : 40g
Mlag Sync : IN_SYNC


#sh mlag domain details
-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number: 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49

Hello RCV State: Current
Hello Periodic Timer State: Fast Periodic
```

```
Domain Sync : IN_SYNC
Neigh Domain Sync : IN_SYNC
Domain Adjacency : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
Mapped Aggregator: po1
Admin Key: 32769
Oper Key: 16385
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync : IN_SYNC
```

Table 5-96 Shows the output details.

Table 5-96: Show mlag summary details

Entry	Description
Domain System Number	Number to identify the node in domain.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Intra domain interface between MLAG domains.
Domain Adjacency	Domain adjacency details and configuration.
Physical properties Digest	physical properties of the digest algorithm.
Total Bandwidth	Total bandwidth available on the interface.
Domain System Number	Number of the domain system.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Details of the intra domain in the interface.
Hello RCV State	State of the hello RCV in the interface.
Hello Periodic Timer State	State of the hello periodic timer in the interface.
Domain Sync	Detail of the domain configuration synchronization.
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.

Table 5-96: Show mlag summary details

Entry	Description
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mcec statistics

Use this command to display all the statistics related to hello and info pdu's in mcec domain.

Command Syntax

```
show mcec statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mcec statistics
Unknown MCCPDU received on the system : 0

-------------------------------------
IDP xe49
-------------------------------------
Valid RX Hello PDUs : 109
Valid TX Hello PDUs : 201
Valid RX Info PDUs: 23
Valid TX Info PDUs : 28
Valid RX Mac Sync PDUs : 5
Valid TX Mac Sync PDUs : 4

MLAG 1
Valid RX Info PDUs : 5
Valid TX Info PDUs : 7
```

Table 5-95 Shows the output details.

Table 5-97: Show mcec statistics details

Entry	Description
RX Hello PDUs	Total number of received hello PDUs.
TX Hello PDUs	Total number of transmitted hello PDUs.
RX Info PDUs	Total number of received Info PDUs.
TX Info PDUs	Total number of transmitted Info PDUs.
RX Mac Sync PDUs	Total number of received Mac Sync PDUs.
TX Mac Sync PDUs	Total number of transmitted Mac Sync PDUs.

show spanning-tree mlag operational-config

Use this command to display the operational information for MC-LAG.

Command Syntax

```
show spanning-tree mlag operational-config
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced before OcNOS-SP version 4.0.

Examples

```
#show spanning-tree mlag operational-config
Operational Configuration
----------------------------------------
Bridge Priority : 32768
Pathcost method : Long
Interface : mlag1
Pathcost : 1000
Priority : 0
```

show spanning-tree mlag sync-detail

Use this command to display the spanning-tree properties shared with the domain peer node.

Command Syntax

```
show spanning-tree mlag sync-detail
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced before OcNOS-SP version 4.0.

Examples

```
#show spanning-tree mlag sync-detail
Domain Digest Parameters
----------------------------------------
Max Age : 20
BPDU Filter : Disabled
BPDU Guard : Disabled
Hello time : 2
Forward Delay : 15
Force Version : 2
Err-disable status : Disabled
Err-disable timeout : 300
MSTP Enabled : Enabled
MSTP Bridge Forward : Disabled
Interface Digest parameters
----------------------------
Port Name : mlag1
Admin Root Guard : Disabled
Admin Edge port : Disabled
Portfast configuration : Disabled
Restricted TCN : Disabled
Admin BPDU filter : Default
Admin BPDU guard : Default
```

switchover type

Use this command to set the MC-LAG switchover type.

Use the no form of this command to turn off switchover.

Command Syntax

```
switchover type revertive <1-255>
switchover type non-revertive
no switchover type (revertive | non-revertive)
```

Parameters

`revertive` If a failure happens that triggers a switchover, after failure recovery the initially-active node becomes active again

`<1-255>` Switch back to the initially-active node this many seconds after failure recovery

non-revertive Do not switch back to the initially-active node after failure recovery

Default

Revertive time as 10 second is the default time.

Command Mode

Privilege exec mode

Applicability

This command was introduced before OcNOS-SP version 4.0.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#switchover type revertive 20
(config)#
(config)#interface mlag1
(config-if)#switchover type non-revertive
```

CHAPTER 6 Traffic Mirroring Commands

This chapter provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

monitor session

Use this command to create a local or remote monitor session. By default, a local monitor session is created.

A monitor session consists of:

- A single destination interface, referred to as a mirror-to port or a single remote destination
- One or more source interfaces (egress, ingress, or both)
- One or more VLAN sources in the ingress direction
- One or more filters that can be applied to filter the mirrored packets

Use the `no` parameter to delete a monitor session.

Command Syntax

```
monitor session <1-18> ( | type ( local | remote ))
no monitor session ( <1-18> | all )
```

Parameters

`<1-18>`	Session number
`local`	Create a local session
`remote`	Create a remote source node session
`all`	All sessions

Default

By default, monitor session type is local and will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 1
(config-monitor)#exit
(config)#monitor session 3 type remote
(config-monitor)#exit
(config)#no monitor session 1
```

monitor session shut

Use this command to deactivate one or all monitor sessions.

Use the no parameter to activate one or all monitor sessions.

Command Syntax

```
monitor session (<1-18> | all) shut
no monitor session (<1-18> | all) shut
```

Parameters

<1-18>	Session number
all	All sessions

Default

Monitor session will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

(config)#no monitor session 3 shut
```

source port

Use this command to configure a source port per monitor session in either ingress or egress or both directions. Source port can be physical interface or a trunk port.

Use the no parameter to remove the source port.

Command Syntax

```
source interface IFNAME ( rx | tx | both | )
no source interface IFNAME ( rx | tx | both | )
```

Parameters

IFNAME	Interface name
rx	Ingress direction
tx	Egress direction
both	Both directions

Default

Source port will be mirrored for both directions if the direction is not specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source interface xe1 both
(config-monitor)#no source interface xe1 tx
```

source vlan

Use this command to configure one or more VLANs as source per monitor session. A VLAN as source will be mirrored only in the ingress direction. Up to 32 VLANs can be configured as source per monitor session.

Use the no parameter to remove vlan source from monitor session.

Command Syntax

```
source vlan VLAN_RANGE
no source vlan VLAN_RANGE
```

Parameters

VLAN_RANGE	VLAN identifier or VLAN identifier range

Default

A trunk port is a member of all VLANs by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source vlan 2
(config-monitor)#source vlan 4-10
(config-monitor)#no source vlan 2-5,10
```

destination port

Use this command to configure a mirror-to port per local monitor session. A destination port can be a physical port or a trunk port.

Use the no parameter to remove the destination port from a local monitor session.

Command Syntax

```
destination interface IFNAME
no destination interface IFNAME
```

Parameters

IFNAME	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe3
(config-if)#switchport
(config-if)#exit
(config)#monitor session 1
(config-monitor)#destination interface xe3
(config-monitor)#no destination interface xe3
```

no shut

Use this command to activate a monitor session

Command Syntax

```
no shut
```

Parameters

None

Default

Monitor session will not be active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

shut

Use this command to de-activate a monitor session.

Command Syntax

```
shut
```

Parameters

None

Default

Monitored session is not active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```

filter

Use this command to add filters to the monitor session. Filters can be applied only in case of ingress mirroring.

Use the no parameter to remove the filter from monitor session.

Command Syntax

```
filter {vlan <2-4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) |
  frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|)
  | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6
  (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}
no filter {vlan <2-4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX |
  XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|)
  (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D |
  A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}
```

Parameters

<2-4094>	VLAN identifier
<0-7>	COS number
XXXX.XXXX.XXXX	MAC address
ETHTYPE	Ethertype
arp	ARP frames
req	Request frames
resp	Response frames
A.B.C.D	Single IP address
A.B.C.D/M	IP addresses with mask
X:X::X:X/M	IPv6 addresses with mask

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#filter cos 3 frame-type arp req sender-ip 2.2.2.1
(config-monitor)#no filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#no filter cos 3 frame-type arp req sender-ip 2.2.2.1
```

description

Use this command to add a description to the monitor session.

Use the no parameter to delete a description of the monitor session.

Command Syntax

```
description LINE
no description
```

Parameters

LINE	Enter the description string

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#description “port mirror rx”
(config-monitor)#no description
```

remote destination

Use this command to configure a destination VLAN and the reflector port for the remote monitor session.

Use the no parameter to remove a destination from a remote monitor session.

Command Syntax

```
destination remote vlan <2-4094> reflector-port IFNAME
no destination remote
```

Parameters

<2-4094>	VLAN identifier
IFNAME	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#no vlan 900 bridge 1
(config)#interface xe3
(config-if)#switchport
(config)#monitor session 1
(config-monitor)#destination remote vlan 900 reflector-port xe3
(config-monitor)#no destination remote
```

show monitor

Use this command to display states of all monitor sessions. If a session is down, the reason is displayed.

Command Syntax

```
show monitor
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor
Session   State          Reason               Description
------- ----------- ---------------------- --------------------------------
1       down        No sources configured
2       down        Dst in wrong mode
```

show monitor session

Use this command to display the configuration details of one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) (brief|)
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)
`brief`	Brief information

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1
session 1
---------------
type              : local
state             : down (Session admin shut)
source intf       :
tx                : xe1 xe3 xe4
rx                : xe2 xe3 xe4
both              : xe3 xe4
source VLANs      :
rx                : 2,5-10,15,18-20
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
#
```

Table 6-98 Explains the show command output fields

Table 6-98: Show monitor session output fields

Field	Description
Type	Type of monitor session.
State	State of the security flow filter.
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).

Field	Description
Both	Incoming and reverse flow (source and destination IP address)
Destination Port	Name of the destination port to be matched.
Source intf	Number of maximum intf central source session.
Source VLANs	Number of maximum VLANs central source session.
Filter count	Used to count number of lines in a file or table.

show filter

Use this command to display filters for one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) filter
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1 filter
session 1
---------------
filter count : 3
---------------

match set 1
---------------
destination mac address : 0000.0002.4451 (host)
source mac address : 0000.0012.2288 (host)
---------------

match set 2
---------------
frame type : arp
sender ip address : 2.2.2.5
target ip addres : 2.2.2.8
---------------

match set 3
---------------
destination mac address : 0000.0001.1453 (host)
frame type : ipv4
source ip address : 3.3.3.5
#
```

show monitor running configuration

Use this command to display the mirror-related running configuration.

Command Syntax

```
show running-config monitor (all|)
```

Parameters

`all`	Show running configuration with defaults

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config monitor
!
monitor session 1
 source interface xe10 rx
 destination interface po1
 no shut

#
```

monitor session shut

Use this command to deactivate one or all monitor sessions.

Use the no parameter to activate one or all monitor sessions.

Command Syntax

```
monitor session (<1-18> | all) shut
no monitor session (<1-18> | all) shut
```

Parameters

<1-18>	Session number
all	All sessions

Default

Monitor session will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

(config)#no monitor session 3 shut
```

show mirror interface <if-name>

Use this command to display mirror interface details.

Command Syntax

```
show mirror interface <if-name>
```

Parameters

IFNAME	Interface name

Default

None.

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mirror interface eth0
Mirror Test Port Name: eth1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: eth0
```

mirror interface <if-name> direction

Use this command to display mirror interface details.

Command Syntax

```
mirror interface <if-name> direction both|receive|transmit
```

Parameters

IFNAME	Interface name
direction	mirroring direction

Default

None.

Command Mode

Interface Config mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#interface eth1
mirror interface eth0 direction both
```

CHAPTER 7 VLAN and Private VLAN Commands

This chapter has the commands used to manage VLANs and Private VLANs. A private VLAN contains switch ports that cannot communicate with each other, but can access other networks. This chapter includes the following commands:

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the no form of this command to remove association of all the secondary VLANs to a primary VLAN.

Command Syntax

```
private-vlan association add VLAN_RANGE
private-vlan association remove VLAN_RANGE
no private-vlan association
```

Parameters

add	Add a VLAN to private VLAN list.
remove	Removes values associated with a single VLAN.
VLAN_RANGE	Specify VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19 of the private VLANs to be configured

Default

By default, functionality is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan association add 3-4
(config-vlan)#private-vlan association remove 3-4
(config-vlan)#no private-vlan association
```

private-vlan community

Use this command to set a VLAN type for a private (community) VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> community bridge <1-32>
no private-vlan <2-4094> community bridge <1-32>
```

Parameters

<2-4094>	Specify a private VLAN identifier.
bridge	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 4 community bridge 1
```

private-vlan isolated

Use this command to create an isolated private VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> isolated bridge <1-32>
no private-vlan <2-4094> isolated bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 3 isolated bridge 1
```

private-vlan primary

Use this command to create a primary VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> primary bridge <1-32>
no private-vlan <2-4094> primary bridge <1-32>
```

Parameters

<2-4094>	Specify a private VLAN identifier.
bridge	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 2 primary bridge 1
```

show vlan

Use this command to display information about static, dynamic or all VLANs.

Command Syntax

```
show vlan (all|static|dynamic|auto) bridge <1-32>
```

Parameters

`<1-32>`	Displays the bridge group ID.
`all`	Displays all VLANs (static and dynamic).
`static`	Displays static VLANs.
`dynamic`	Displays dynamic VLANs.
`auto`	Displays auto configured VLANs.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Up         xe2(u) xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t) xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t) xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up         xe10(t)
#
```

Table 7-99 Explains the show command output fields.

Table 7-99: show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.

Field	Description
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan brief

Use this command to display brief VLAN information for all bridges.

Command Syntax

```
show vlan (brief | <2-4094>)
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from this command when using the `all` parameter.

```
#show vlan brief

Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ======= ==============================
1               1       default          ACTIVE  eth2(u)


0               1       default          ACTIVE
0               2       new              ACTIVE
```

Table 7-100 Explains the show command output fields.

Table 7-100: show vlan brief output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan classifier

Use this command to display information on configured VLAN classifier groups, interfaces configured for a VLAN group or all the groups, or all configured VLAN classifier rules.

If either a group ID or rule ID is not specified, all configured VLAN classifier rules are shown. If either a group ID or rule ID is specified, a specific configured VLAN classifier rule is shown.

Command Syntax

```
show vlan classifier group interface IFNAME
show vlan classifier group (<1-16>|)
show vlan classifier rule(<1-256>|)
```

Parameters

`group`	Displays group activated information.
`<1-16>`	Displays the group ID
`interface`	Displays interface information.
`interface`	Displays interface group information.
`group`	Displays group activated information.
`<1-16>`	Displays the group ID.
`rule`	Displays VLAN classifier rule ID.
`<1-256>`	Displays rule ID information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example displays groups for VLAN classifier groups:

```
#show vlan classifier group 1
vlan classifier group 1 add rule 1
```

This example displays interfaces for all VLAN classifier groups:

```
#show vlan classifier interface group
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
vlan classifier group 2 interface fe5
vlan classifier group 3 interface fe7
```

This example displays interfaces for VLAN classifier group 1:

```
#show vlan classifier interface group 1
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
```

This example displays interfaces for VLAN classifier rule 1:

```
#show vlan classifier rule 1
vlan classifier rule 1 mac 222.2222.2222 vlan 2
```

switchport access

Use this command to change the default VLAN on the current interface.

Note: IP Infusion Inc. does not recommend using VLAN identifier 1 because of interoperability issues with other vendors' equipment.

Use the no parameter to remove an existing VLAN.

Command Syntax

```
switchport access vlan <2-4094>
no switchport access vlan
```

Parameter

<2-4094>	Specify the VLAN identifier.

Default

The switchport access vlan default value is 3968.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
#configure terminal
(config)#interface eth0
(config-if)#switchport access vlan 3

(config)#interface eth0
(config-if)#no switchport access vlan
```

switchport hybrid

Use this command to set the switching characteristics of the interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the no parameter to turn off allowed hybrid switching.

Command Syntax

```
switchport hybrid allowed vlan all
switchport hybrid vlan <2-4094>
switchport hybrid allowed vlan none
switchport hybrid allowed vlan except VLAN_ID
switchport hybrid allowed vlan remove VLAN_ID
switchport hybrid allowed vlan add VLAN_ID egress-tagged (enable|disable)
no switchport hybrid
no switchport hybrid vlan
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`except`	Allow all VLANs except these VLANs to transmit and receive through the interface.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`egress-tagged`	Whether to tag outgoing frames.
`enable`	Enable egress tagging for outgoing frames.
`disable`	Disable egress tagging for outgoing frames.

Default

By default, switchport hybrid is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2 egress-tagged enable
```

The following shows adding a range of VLANs to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2-4 egress-tagged enable
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Command Syntax

```
switchport mode (access|hybrid|trunk|provider-network|customer-edge
|customer-network|private-vlan)
```

Parameters

`access`	Access.
`hybrid`	Hybrid.
`trunk`	Trunk.
`provider-network`	Provider network.
`customer-network`	Customer network.

Default

By default, switchport hybrid is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access
```

switchport mode access ingress-filter

Use this command to set the switching characteristics of the interface to access mode, and classify untagged frames only. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode access ingress-filter (enable|disable)
```

Parameters

`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access ingress-filter enable
```

switchport mode hybrid acceptable-frame-type

Use this command to set the interface acceptable frame types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

`all`	Set all frames can be received
`vlan-tagged`	Accept only classified frames that belong to the port's member set.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid acceptable-frame-type vlan-tagged
```

switchport mode hybrid ingress-filter

Use this command to set the switching characteristics of the interface as hybrid, and classify both tagged and untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode hybrid ingress-filter (enable|disable)
```

Parameters

`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid ingress-filter enable
```

switchport mode trunk ingress-filter

Use this command to set the switching characteristics of the interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode trunk ingress-filter (enable|disable)
```

Parameters

`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode trunk ingress-filter enable
```

switchport trunk allowed

Use this command to set the switching characteristics of the interface to trunk.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the no parameter to remove all VLAN identifiers configured on this port.

Command Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLAN_ID
switchport trunk allowed vlan except VLAN_ID
switchport trunk allowed vlan remove VLAN_ID
no switchport trunk
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`except`	All VLANs except these VLANs are part of the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2-4
```

switchport trunk native

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the no parameter to revert the native VLAN to the default VLAN identifier 1.

Command Syntax

```
switchport trunk native vlan VLAN_ID
no switchport trunk native vlan
```

Parameter

VLAN_ID	VLAN identifier(s) <1-4094>. You can specify a single VLAN, or a VLAN list. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces in between the hyphens or commas.

Default

The default is that ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport trunk native vlan 2

(config)#interface eth0
(config-if)#no switchport trunk native vlan
```

switchport mode private-vlan

Use this command to make a Layer 2 port a host port, promiscuous port, or trunk port.

Use the no form of this command to remove the configuration.

Command Syntax

```
switchport mode private-vlan (host | promiscuous)
no switchport mode private-vlan (host | promiscuous)
```

Parameters

host	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
promiscuous	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN

Default

By default, switchport mode private-vlan is host.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode private-vlan host
(config)#interface eth1
(config-if)#switchport mode private-vlan promiscuous
(config)#interface eth2
(config-if)#no switchport mode private-vlan promiscuous
```

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the no form of this command to remove the association.

Command Syntax

```
switchport private-vlan host-association <2-4094> add <2-4094>
no switchport private-vlan host-association
```

Parameters

<2-4094>	VLAN identifier of the primary VLAN.
add	Adds the secondary VLAN.
<2-4094>	VLAN identifier of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan host-association 2 add 3

#configure terminal
(config)#interface eth0
(config-if)#no switchport private-vlan host-association
```

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the no form of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Command Syntax

```
switchport private-vlan mapping <2-4094> add VLAN_ID
switchport private-vlan mapping <2-4094> remove VLAN_ID
no switchport private-vlan mapping
```

Parameters

<2-4094>	VLAN identifier of the primary VLAN.
add	Adds the secondary VLAN.
remove	Removes the secondary VLAN.
VLAN_ID	VLAN identifier <2-4094> of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan mapping value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan mapping 2 add 3-4
(config-if)#switchport private-vlan mapping 2 remove 3-4

(config-if)#no switchport private-vlan mapping
```

vlan classifier activate

Use this command to activate the VLAN classifier.

Use no form of this command to deactivate the VLAN classifier.

Command Syntax

```
vlan classifier activate <1-16> vlan <2-4096>
no vlan classifier activate <1-16>
```

Parameters

<1-16>	Indicates the VLAN classifier activate identifier.
<2-4094>	VLAN identifier of the primary VLAN.

Default

By default, vlan classifier activate value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth2
(config-if)#vlan classifier activate 1 vlan 2

(config-if)#no vlan classifier activate 1
```

vlan classifier group

Use this command to create a subnet-based VLAN classifier group. A group indicates a VLAN classifier group ID.

Command Syntax

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

Parameters

`add`	Adds a rule to a group.
`delete`	Deletes a rule from a group.
`rule`	Indicates the VLAN classifier rule identifier `<1-256>`.

Default

By default, vlan classifier group value is 1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier group 1 delete rule 1
(config)#no vlan classifier group 2
```

vlan classifier rule ipv4

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> ipv4 A.B.C.D/M
no vlan classifier rule <1-256>
```

Parameters

A.B.C.D/M	Indicates the IPv4 address classification. Enter the address in A.B.C.D/M format.

Default

By default, vlan classifier rule is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 ipv4 20.20.20.2/24
(config)#no vlan classifier rule 2
```

vlan classifier rule mac

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN.

If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> mac WORD
no vlan classifier rule <1-256>
```

Parameters

WORD	Indicate the Mac address classification. Enter the address in HHHH.HHHH.HHHH format.

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 mac fe80::22e::b5ff:fee8:6/64
(config)#no vlan classifier rule 2
```

vlan classifier rule proto

Use this command to create a subnet-based VLAN classifier rule for a protocol and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> proto (ip|ipv6|ipx|x25|arp|rarp|atalkddp|atalkaarp|
  atmmulti|atmtransport|pppdiscovery|pppsession|xeroxpup|xeroxaddrtrans|g8bpqx25|
  ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnaremoteconsole|decdnarouting|
  declat|decdiagnostics|deccustom|decsyscomm|<0-65535>)
no vlan classifier rule <1-256>
```

Parameters

`<0-65535>`	Ethernet decimal
`arp`	Address Resolution Protocol
`atalkaarp`	Appletalk AARP
`atalkddp`	Appletalk DDP
`atmmulti`	MultiProtocol Over ATM
`atmtransport`	Frame-based ATM Transport
`dec`	DEC Assigned
`deccustom`	DEC Customer use
`decdiagnostics`	EC Diagnostics
`decdnadumpload`	DEC DNA Dump/Load
`decdnaremoteconsole`	DEC DNA Remote Console
`decdnarouting`	DEC DNA Routing
`declat`	DEC LAT
`decsyscomm`	DEC Systems Comms Arch
`g8bpqx25`	G8BPQ AX.25
`ieeeaddrtrans`	Xerox IEEE802.3 PUP Address Translation
`ieeepup`	Xerox IEEE802.3 PUP
`ip`	IP address
`ipv6`	IPv6 address
`ipx`	IPX address
`pppdiscovery`	PPPoE discovery
`pppsession`	PPPoE session
`rarp`	Reverse Address Resolution
`x25`	CCITT X.25
`xeroxaddrtrans`	Xerox PUP Address Translation
`xeroxpup`	Xerox PUP

`ethv2`	Ethernet v2
`nosnapllc`	Indicates LLC without snap encapsulation
`snapllc`	Indicates LLC snap encapsulation

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 proto ip
(config)#no vlan classifier rule 2
```

vlan database

Use this command to enter the VLAN configuration mode to add, delete, or modify values associated with a single VLAN.

Command Syntax

```
vlan database
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

vlan state

This command enables or disables the state of a particular VLAN on the bridge.

Command Syntax

```
vlan <2-4094> bridge <1-32> (state (enable|disable)|)
```

Parameters

`<1-32>`	Specify bridge group ID
`state`	Indicates the operational state of the VLAN
`enable`	Sets VLAN into a enable state.
`disable`	Sets VLAN into a disable state.
`name`	The VLAN name
`WORD`	The name of the VLAN

Default

By default, vlan bridge state is disabled.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 45 bridge 1 state enable
```

vlan VLAN_RANGE bridge

.This command allows you to create a single/range of VLAN’s on the VLAN aware bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE bridge <1-32>
vlan VLAN_RANGE bridge <1-32> (name WORD|) state (enable | disable)
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

VLAN_RANGE	The vlan-id or range of vlan-id's separated by ','&'-'
bridge	Specify the bridge group ID in the range <1-32>.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state.

Default

By default, vlan bridge state is disabled

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan 3-40,56 bridge 4
(config)#no vlan 2-5 bridge 2
```

CHAPTER 8 802.1x Commands

This chapter provides a description, syntax, and examples of the 802.1X commands. It includes the following commands:

auth-mac disable

Use this command to disable MAC authentication on an interface. See the auth-mac enable command to enable MAC authentication on a interface.

Command Syntax

```
auth-mac disable
```

Parameters

`disable`	Disable MAC authentication on an interface.

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable
```

auth-mac enable

Use this command to enable MAC authentication on an interface. See the auth-mac disable command to disable MAC authentication on an interface.

Command Syntax

```
auth-mac enable
```

Parameters

`enable`	Enable MAC authentication on an interface.

Default

By default, MAC authentication is globally disabled on the device.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable
```

auth-mac system-auth-ctrl

Use this command to enable MAC authentication globally. If MAC authentication is not enabled, other MAC authentication related commands throw an error when issued.

Use the no parameter with this command to disable MAC authentication globally.

Command Syntax

```
auth-mac system-auth-ctrl
no auth-mac system-auth-ctrl
```

Parameters

None

Default

Authentication system messages are not displayed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#auth-mac system-auth-ctrl

(config)#no auth-mac system-auth-ctrl
```

debug dot1x

Use this command to turn on or turn off 802.1x debugging at various levels.

Use the no parameter with this command or the undebug command to turn off debugging.

Command Syntax

```
debug dot1x (all|)
debug dot1x event
debug dot1x nsm
debug dot1x packet
debug dot1x timer
no debug dot1x (all|)
no debug dot1x event
no debug dot1x nsm
no debug dot1x packet
no debug dot1x timer
undebug dot1x (all|)
undebug dot1x event
undebug dot1x packet
undebug dot1x nsm
undebug dot1x timer
```

Parameters

all	Sets debugging for all 802.1x levels.
event	Sets debugging for 802.1x events.
nsm	Sets debugging for 802.1x NSM information.
packet	Sets debugging for 802.1x packets.
timer	Sets debugging for 802.1x timer.

Default

No default value is specified.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dot1x all
(config)#debug dot1x event
```

dot1x port-control

Use this command to force a port state.

Use the no parameter with this command to remove a port from the 802.1x management.

Command Syntax

```
dot1x port-control (force-unauthorized|force-authorized|auto)
no dot1x port-control
```

Parameters

`auto`	Specify to enable authentication on port.
`force-authorized`	Specify to force a port to always be in an authorized state.
`force-unauthorized`	Specify to force a port to always be in an unauthorized state.

Default

The dot1x port-control default is active.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x port-control auto

(config)#interface eth0
(config-if)#no dot1x port-control
```

dot1x protocol-version

Use this command to set the protocol version of dot1x to 1 or 2. The protocol version must be synchronized with the Xsupplicant being used in that interface.

Use the no parameter with this command to set the protocol version to the default value (2).

Command Syntax

```
dot1x protocol-version <1-2>
no dot1x protocol-version
```

Parameters

<1-2>	Indicates the EAP Over LAN (EAPOL) version.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x protocol-version 2

(config)#interface eth0
(config-if)#no dot1x protocol-version
```

dot1x quiet-period

Use this command to set the quiet-period time interval.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By administratively changing the quiet-period interval, by entering a lower number than the default, a faster response time can be provided.

Use the no parameter with this command to set the configured quiet period to the default (60 seconds).

Command Syntax

```
dot1x quiet-period <1-65535>
no dot1x quiet-period
```

Parameter

<1-65535>	Seconds between the retrial of authentication.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x quiet-period 200
```

dot1x reauthMax

Use this command to set the maximum reauthentication value, which sets the maximum number of reauthentication attempts after which the port will be unauthorized.

Use the no parameter with this command to set the reauthentication maximum to the default value (2).

Command Syntax

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

Parameter

<1-10>	Indicates the maximum number of reauthentication attempts after which the port will be unauthorized.

Default

The default is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sets the maximum reauthentication value to 5.

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthMax 5
```

The following sets the reauthentication maximum to the default value.

```
#configure terminal
(config)#interface eth0
(config-if)#no dot1x reauthMax
```

dot1x reauthentication

Use this command to enable reauthentication on a port.

Use the no parameter to disable reauthentication on a port.

Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

Parameters

None

Default

The dot1x reauthentication default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthentication
```

dot1x system-auth-ctrl

Use this command to enable globally authentication.

Use the no parameter to disable globally authentication.

Command Syntax

```
dot1x system-auth-ctrl
no dot1x system-auth-ctrl
```

Parameters

None

Default

Authentication is off by default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#dot1x system-auth-ctrl
```

dot1x timeout re-authperiod

Use this command to set the interval between reauthorization attempts.

Use the no parameter to disable the interval between reauthorization attempts.

Command Syntax

```
dot1x timeout re-authperiod <1-4294967295>
no dot1x timeout re-authperiod
```

Parameter

`<1-4294967295>` Specify the seconds between reauthorization attempts.

Default

Default time is 3600 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout re-authperiod 25
```

dot1x timeout server-timeout

Use this command to set the authentication sever response timeout.

Use the no parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

Parameter

<1-65535>	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout server-timeout 555

(config)#interface eth0
(config-if)#no dot1x timeout server-timeout
```

dot1x timeout supp-timeout

Use this command to set the interval for a supplicant to respond.

Use the no parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

Parameter

<1-65535>	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout supp-timeout 40

(config)#interface eth0
(config-if)#no dot1x timeout supp-timeout
```

dot1x timeout tx-period

Use this command to set the interval between successive attempts to request an ID.

Use the no parameter to disable the interval between successive attempts to request an ID.

Command Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter

<1-65535>	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout tx-period 34

(config)#interface eth0
(config-if)#no dot1x timeout tx-period
```

ip radius source-interface

Use this command to set the local address sent in packets to the radius server.

Use the no parameter to clear the local address.

Command Syntax

```
ip radius source-interface IP-address PORT
no ip radius source-interface
```

Parameters

IP-address	RADIUS client dotted IP address.
PORT	Specify the radius client port number. The default port number is 1812.

Default

The default port number is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip radius source-interface 12.12.12.1 1812

(config)#no ip radius source-interface
```

radius-server dot1x host

Use this command to specify the IP address of the remote radius server host and assign authentication and accounting destination port numbers. Multiple radius-server host commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host.

If the auth-port parameter is not specified, it will take the default value of the auth-port. If you do not specify the auth-port to unconfigure, and the default value of the auth-port does not match the port you are trying to unconfigure, the specified radius-server host will not be unconfigured.

Use the no form of the command to unconfigure a specified radius-server.

Command Syntax

```
radius-server dot1x host (A.B.C.D)(|(key ((0 WORD) | (7 WORD) | (WORD))(|(auth-port
  <0-65535> (|(timeout <1-60> (|(retransmit <1-100>)))))))
no radius-server dot1x host (A.B.C.D)(|(key ((0 WORD) | (7 WORD)
| (WORD))(|(auth-port <0-65535> (|(timeout (|(retransmit <1-100>)))))))
```

Parameters

dot1x	IEEE 802.1X Port-Based Access Control.
A.B.C.D	IPv4 address of the RADIUS server.
auth-port	RADIUS server's port for authentication.
key	Specify the global shared key.
retransmit	Global RADIUS server retransmit count.
timeout	Specify the RADIUS server timeout(default: 5 seconds).
0	To specify shared key in clear-text form.
7	To specify shared key in encrypted form.
WORD	RADIUS shared secret(clear text) (Max Size 63).
<0-65535>	Port number.
<0-100>	Global RADIUS server retransmit count.
<1-60>	RADIUS server timeout period in seconds.

Default

The default value of auth-port is 1645.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x host 12.12.12.1 auth-port 1233 timeout 1
retransmit 2

(config)#no radius-server dot1x host 12.12.12.1 auth-port 1233
```

radius-server dot1x retransmit

Use this command to specify the number of times the router transmits each radius request to the server before giving up.

Use the no form of this command to disable retransmission.

Command Syntax

```
radius-server dot1x retransmit RETRIES
no radius-server dot1x retransmit
```

Parameter

dot1x	IEEE 802.1X Port-Based Access Control.
RETRIES	Specify the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

Default

The default value is 3.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x retransmit 12

(config)#no radius-server dot1x retransmit
```

radius-server dot1x timeout

Use this command to specify the number of seconds a router waits for a reply to a radius request before retransmitting the request.

Use the no parameter to use the default value.

Command Syntax

```
radius-server dot1x timeout <1-60>
no radius-server dot1x timeout
```

Parameter

dot1x	IEEE 802.1X Port-Based Access Control.
<1-60>	RADIUS server timeout period in seconds.

Default

The default value is 5 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x timeout 20

#configure terminal
(config)#no radius-server dot1x timeout
```

show debugging dot1x

Use this command to display the status of the debugging of the 802.1x system.

Command Syntax

```
show debugging dot1x
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging dot1x
802.1X debugging status:
```

show dot1x

Use this command to display the state of the whole system.

Command Syntax

```
show dot1x
show dot1x all
show dot1x diagnostics interface IFNAME
show dot1x interface IFNAME
show dot1x sessionstatistics (interface IFNAME|)
show dot1x statistics interface IFNAME
```

Parameters

`all`	Display all information.
`diagnostics`	Display diagnostics information.
`interface`	Display diagnostics interface information.
`interface`	Display interface information.
`sessionstatistics`	Display session statistics.
`interface`	Display session statistics interface information.
`statistics`	Display statistics information.
`interface`	Display statistics interface information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Displayed Output

The following tables describes the output for the show dot1x all command and the show dot1x interface command.

Table 8-101: Port variables

Entry	Description
portEnabled	Interface operational status (Up-true/down-false)
portControl	Current control status of the port for 802.1x control
portStatus	802.1x status of the port (authorized/unauthorized)
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Value holds meaning only if reAuthentication is enabled

Table 8-102: Supplicant PAE related global variables

Entry	Description
abort	Indicates that authentication should be aborted when set to true
fail	Indicates failed authentication attempt when set to false
start	Indicates authentication should be started when set to true
timeout	Indicates authentication attempt timed out when set to true
success	Indicates authentication successful when set to true

Table 8-103: 802.1x Operational State of Interface

Entry	Description
mode	Configured 802.1x mode
reAuthCount	Reauthentication count
quietperiod	Time between reauthentication attempts
reAuthMax	Maximum reauthentication attempts

Table 8-104: Backend Authentication state machine variables and constants

Entry	Description
state	State of the state machine
reqCount	Count of requests sent to server
suppTimeout	Supplicant timeout
serverTimeout	Server timeout
maxReq	Maximum requests to be sent

Table 8-105: Controlled Directions State machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)
operControlledDirections	Operational Value (Both/In)

Table 8-106: KR -- Key receive state machine

Entry	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 8-107: Key Transmit State machine

Entry	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the state of the system.

```
#show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
```

The following is an output of this command displaying detailed information for all ports.

```
#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
%  portEnabled: true - portControl: auto
%  portStatus: unauthorized - currentId: 11
%  reAuthenticate: disabled
%  abort:F fail:F start:F timeout:F success:F
%  PAE: state: connecting - portMode: auto
%  PAE: reAuthCount: 2 - rxRespId: 0
%  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
%  BE: state: idle - reqCount: 0 - idFromServer: 0
%  BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
%  CD: adminControlledDirections: in - operControlledDirections: in
%  CD: bridgeDetected: false
%  KR: rxKey: false
%  KT: keyAvailable: false - keyTxEnabled: false
```

CHAPTER 9 Layer 2 Subinterface Commands

This chapter is a reference for the Layer 2 subinterface commands.

cross-connect

Use this command to create an AC-to-AC cross-connect between the L2 subinterfaces. It creates a separate mode with endpoint1 and endpoint2 being L2 subinterfaces. It is possible to bind L2 subinterface to cross-connect only when encapsulation is configured on it.

Use the no form of this command to remove the given cross-connect.

Command Syntax

```
cross-connect <WORD> (interface <IFNAME>) (interface <IFNAME>) (description)
  (disable)
no cross-connect <WORD>
```

Parameters

WORD	XC name
IFNAME	AC interface name
description	Characters describing AC cross-connect
disable	disables the cross-connect

Default

None

Command Mode

Configure mode for cross-connect

Cross-connect mode for IFNAME, description and disable

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#cross-connect c1
(config-xc)#interface xe1.1
(config-xc)#interface xe1.2
(config-xc)#description XC1
(config-xc)#disable
(config-xc)#exit
(config)#no cross-connect c1
(config)#
```

encapsulation

Use this command to configure encapsulation-type for a L2 subinterface. With this command, a Layer 2 subinterface can be configured as single-tagged with single/multiple vlans or double-tagged, or default or untagged. Operational state of the layer 2 subinterface is DOWN before configuring the encapsulation and it becomes UP once the encapsulation is configured.

Use the no form of this command to unconfigure the encapsulation.

Command Syntax

```
encapsulation ((dot1q | dot1ad | default | untagged) (vlan-id | vlanid-range)
  (inner-dot1q vlan-id))
no encapsulation
```

Parameters

dot1q	IEEE802.1Q VLAN-tagged packets
dot1ad	IEEE802.1ad VLAN-tagged packets
default	IEEE default packets
untagged	IEEE untagged packets
VLAN_RANGE	VLAN ID 2-4094 or range(s): 2-5 10 or 2-5 7-19
inner-dot1q	Inner-VLAN for double-tagged

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 10
(config-if)#ex
(config)#interface xe1.2 switchport
(config-if)#encapsulation dot1ad 11
(config-if)#ex
(config)#interface xe1.3 switchport
(config-if)#encapsulation default
(config-if)#ex
(config)#interface xe1.4 switchport
(config-if)#encapsulation untagged
(config-if)#ex
(config)#interface xe1.5 switchport
(config-if)#encapsulation dot1q 15-20
(config-if)#ex
(config)#interface xe1.6 switchport
```

```
(config-if)#encapsulation dot1ad 21-25
(config-if)#ex
(config)#interface xe1.7 switchport
(config-if)#encapsulation dot1q 100 inner-dot1q 10
(config-if)#ex
(config)#interface xe1.8 switchport
(config-if)#encapsulation dot1ad 200 inner-dot1q 20
(config-if)#ex
(config)#interface xe1.1 switchport
(config-if)#no encapsulation
(config-if)#ex
(config)#
```

interface IFNAME.SUBINTERFACE_ID switchport

Use this command to configure a L2 subinterface. An L2 sub-interfaces makes it possible for a logical interface to be created on an Ethernet physical interface as well as on dynamic/static LAG interfaces to handle one slice of its resource. The supported method for this resource slicing is vlan credential based which can be a single tagged or double-tagged or untagged or default along with encapsulation types as either dot1q or dot1ad.

Use no form of this command to unconfigure a sub-interface.

Command Syntax

```
interface IFNAME.SUBINTERFACE_ID switchport
no interface IFNAME.SUBINTERFACE_ID
```

Parameters

IFNAME	Interface name, such as xe1, po1 or sa1
SUBINTERFACE_ID	Subinterface identifier <1-2000>
switchport	L2 subinterface

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#exit
(config)#no interface xe1.1
(config)#interface po1.1 switchport
(config-if)#exit
(config)#no interface po1.1
(config)#interface sa1.1 switchport
(config-if)#exit
(config)#no interface sa1.1
(config)#exit
#
```

rewrite

Use this command to manipulate the VLAN tags in the incoming packet. Supported operations are PUSH, POP and TRANSLATE on the outer vlan tag with any of these ethertype – 8100/ 88a8/ 9100/ 9200.

Use the no form of this command to unconfigure rewrite.

Command Syntax

```
rewrite ((pop| push | translate) (TPID_VALUE) (VID_RANGE))
no rewrite
```

Parameters

pop	Pop the outer vid
push	Push the outer vid
translate	Translate the outer vid
VALUE	Set service tpid value as 0x8100/0x88a8/0x9100/0x9200
VID_RANGE	<2-4094>

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#rewrite pop
(config-if)#exit
(config)#interface xe1.2 switchport
(config-if)#rewrite push 9100 3
(config-if)#exit
(config)#interface xe1.10 switchport
(config-if)#rewrite translate 9200 4
(config-if)#exit
(config)#interface xe1.1 switchport
(config-if)#no rewrite
(config-if)#ex
```

show cross-connect

Use this command to display the cross-connected subinterfaces along with their status and total number of cross-connects configured in the system.

Command Syntax

```
show cross-connect <WORD>
```

Parameters

WORD	Cross-connect name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show cross-connect
cross-connect status
XC name                         Ep1              Ep2              Status
-------------------------------+----------------+----------------+-------
c1                              xe1.1            xe1.2            UP
-------------------------------+----------------+----------------+-------
AC cross-connect summary
Total : 1
Up    : 1
Down  : 0
#show cross-connect c1
cross-connect status
XC name                         Ep1              Ep2              Status
-------------------------------+----------------+----------------+-------
c1                              xe1.1            xe1.2            UP
-------------------------------+----------------+----------------+-------
```

switchport dot1q ethertype

Use this command to configure the service-tpid value on parent port of a subinterface. By this the tpid used for service tag for a subinterface may be inherited from the one applied to parent interface.

Use no form of this command to revert the value to default.

Note: For any dot1ad subinterface to be functional, switchport dot1q ethertype should be set to desired value as 88a8/9100/9200.

Command Syntax

```
switchport dot1q ethertype (8100 | 88a8 | 9100 | 9200)
no switchport dot1q ethertype
```

Parameters

ETHERTYPE	Physical Interface name. Ethertype value (in 0xhhhh hexadecimal notation. Allowed ethertype values are 0x8100 (default) or 0x88a8 0r 0x9100 or 0x9200)

Default

Default value is 8100

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface xe1
(config-if)#switchport dot1q ethertype 9100
(config-if)#exit
(config)#interface xe1
(config-if)#no switchport dot1q ethertype
(config-if)#exit
```

no subinterfaces

Use this command to unconfigure all the subinterfaces of any type (layer 2 or layer 3) created under a parent port.

Command Syntax

```
no subinterfaces
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface xe1
(config-if)#no subinterfaces
(config-if)#exit
```

CHAPTER 10 Port Security Commands

This chapter describes the port security commands.

port-security

Use this command to enable or disable port security globally.

Command Syntax

```
port-security (enable | disable)
```

Parameters

`enable`	Enable port security globally
`disable`	Disable port security globally

Default

By default, port security is enabled globally.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
(config)#port-security enable
(config)#
```

show port-security

Use this command to display the port security configuration for all interfaces or for a particular interface.

Command Syntax

```
show port-security (interface IFNAME |)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#show port-security
Port port-security mode MAC limit CVLAN SVLAN static secure MAC
-----------------------------------------------------------------
ge1  dynamic            3         2           0000.0000.1112
                                  10          0000.0000.3333

#show port-security interface ge1
Port Security Mode : Dynamic
Secure MAC limit : 3
Static Secure MAC list :
CVLAN SVLAN MAC Address
--------------------------
2           0000.0000.1112
10          0000.0000.3333
```

switchport port-security

Use this command to enable port security on an interface.

Use the no form of this command to disable port security on an interface. This command removes configured secured MAC, if any, on this interface.

Note: These commands are supported for physical, LAG, and MLAG (active) interfaces only. Enabling port security on an interface removes learned MAC addresses of interfaces (whether learned by static or dynamic means), and then relearns the secure MAC addresses. Multicast MAC addresses are not considered as part of the MAC learning limit.

Command Syntax

```
switchport port-security (static |)
no switchport port-security
```

Parameters

`static`	Static mode

Default

By default this feature is disabled; the default mode of port security is to dynamically learn. In dynamic mode, devices learn MAC addresses dynamically. You can program static MACs, however, dynamic MAC learning will not be allowed in static mode for port security.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode hybrid
(config-if)#switchport hybrid allowed vlan all
(config-if)#switchport port-security
```

switchport port-security logging

Use this command to enable violated MAC logging on a port security enabled interface.

Use the `disable` parameter with this command to disable violated mac logging on a port security enabled interface.

Command Syntax

```
switchport port-security logging (enable | disable)
```

Parameters

`enable`	Enable violated MAC logging
`disable`	Disable violated MAC logging

Default

By default logging is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security logging enable
```

switchport port-security mac-address

Use this command to add static secure MAC addresses.

Use the no form of this command to remove static secure MAC addresses.

Command Syntax

```
switchport port-security mac-address XXXX.XXXX.XXXX
no switchport port-security mac-address XXXX.XXXX.XXXX
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
```

Parameters

`XXXX.XXXX.XXXX`	Static secure MAC address
`vlanId`	VLAN identifier
`<2-4094>`	VLAN identifier
`svlanId`	SVLAN identifier
`<2-4094>`	SVLAN identifier

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security mac-address 0000.0000.1112 vlan 2
```

switchport port-security maximum

Use this command to set the MAC address learning limit for an interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. When a newly configured maximum learn limit is less than the previous value, you must remove/flush-out the unwanted MACs to stop traffic forwarding from the unwanted source MAC addresses. MAC addresses can be removed using the clear mac address-table command.

Command Syntax

```
switchport port-security maximum <1-1000>
```

Parameters

<1-1000>	Maximum MAC address learning limit

Default

The default MAC address learning limit is 1.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface po1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface mlag1
(config-if)#switchport port-security maximum 3
```

SECTION 6 # Layer 3

Layer 3 Unicast Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 BGP

This chapter contains basic Border Gateway Protocol configuration examples.

Enable BGP Routers in the Same Autonomous System

Figure 1-57 shows the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS200, connecting to network 10.10.10.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

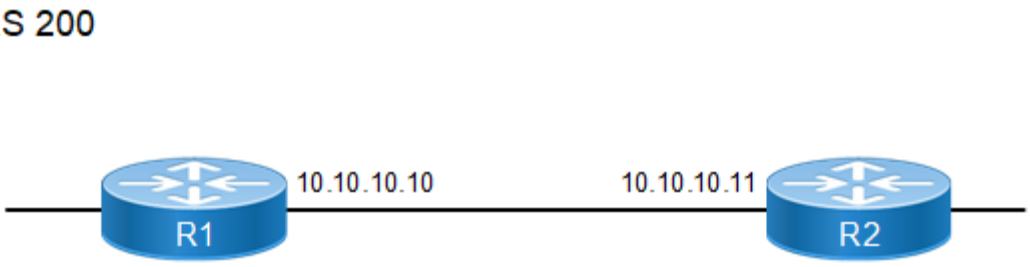


Figure 1-57: Routers in the Same Autonomous System

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `200` is the neighbor's AS number.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.

Validation

```
#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down    State/PfxRcd
10.10.10.11              4    200   387        390       1       0       0
00:00:04               0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 10.10.10.11, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:41
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.10, Local port: 179
Foreign host: 10.10.10.11, Foreign port: 33931
Nexthop: 10.10.10.10
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Enable BGP Between Different Autonomous Systems

This example shows the minimum configuration required for enabling BGP on an interface, when the routers belong to different autonomous systems. R1 and R2 are two routers in different autonomous system, AS200 and AS300, connecting to network 10.10.10.0/24.

Topology

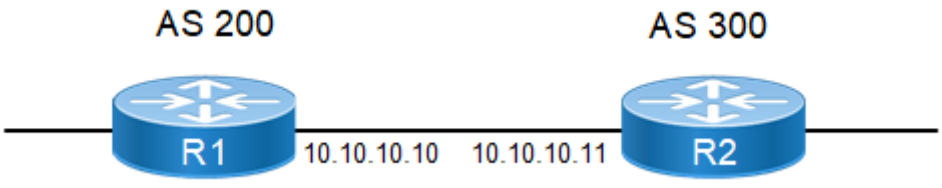


Figure 1-58: Routers in Different Autonomous Systems

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remote-as 300`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `300` is the neighbor's AS number.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 300`	Define the routing process. The number `300` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.

Validation

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:00:15
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.11, Local port: 56091
Foreign host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 300
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down    State/PfxRcd
10.10.10.10              4    200     3          3       1       0       0
00:00:50                0

Total number of neighbors 1

Total number of Established sessions 1
```

Route-Map

Use route maps to filter incoming updates from a BGP peer. In this example, the prefix-list ABC on R1 is configured to deny entry of any routes with the IP address 1.1.1.0/M (M = 26, 27, 28). To test the filter, R2 is configured to generate network addresses 1.1.1.0/27 and 1.1.2.0/24. To verify, use the `show ip bgp` command on R1; it displays R1 receiving updates from only 1.1.2.0/24.

Topology

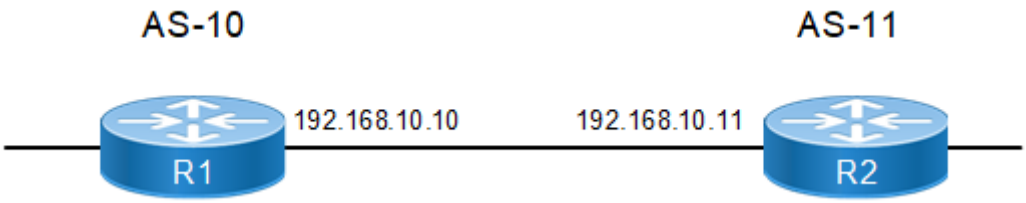


Figure 1-59: Configure Route-Map

R1

`#configure terminal`	Enter configure mode.
`(config)#ip prefix-list ABC seq 5 deny 1.1.1.0/24 ge 26 le 28`	Create an entry in the prefix-list. The ABC parameter is the name of the map that is created above. 5 specifies the sequence number or position of this specific route map. deny specifies the packets are to be rejected. 26 and 28 are the minimum and maximum prefix lengths to be matched.
`(config)#ip prefix-list ABC seq 10 permit any`	Create another entry in the ABC map. 10 specifies the sequence number or position of this specific route map. The permit parameter any specifies accept all packets of any length.
`(config)#route-map ABC permit 1`	Enter Route-map mode to set the match operation.
`(config-route-map)#match ip address prefix-list ABC`	Set the match criteria. In this case, if the route-map name matches ABC, the packets from the first sequence are denied.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 10`	Define the routing process, and establish a TCP session. The number 10 specifies the AS number of R1.
`(config-router)#neighbor 192.168.10.11 remote-as 11`	Define BGP neighbors, and establish a TCP session. 192.168.10.11 is the IP address of the neighbor (R2), and 11 is the neighbor's AS number.

(config-router)#neighbor 192.168.10.11 route-map ABC in	Apply a route map to routes. 192.168.10.11 specifies the IP address of BGP neighbor. The ABC parameter is the name of the route map, and in specifies that the access list applies to incoming advertisements.
(config-router)#exit	Exit router mode.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 1.1.1.1/27 secondary	Specify the interface address.
(config-if)#ip address 1.1.2.1/24 secondary	Specify the interface address.
(config-if)#exit	Exit loopback interface mode.
(config)#router bgp 11	Define the routing process, and establish a TCP session. The number 11 specifies the AS number of R2.
(config-router)#neighbor 192.168.10.10 remote-as 10	Define BGP neighbors, and establish a TCP session. 192.168.10.10 is the IP address of the neighbor (R1), and 10 is the neighbor's AS number.
(config-router)#network 1.1.1.0/27	Specify the network to be advertised by the BGP routing process.
(config-router)#network 1.1.2.0/24	Specify the network to be advertised by the BGP routing process.
(config-router)#exit	Exit router mode.

Validation

```
#show  ip bgp
BGP table version is 2, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.2.0/24       192.168.10.11         0         100           0       11
i

Total number of prefixes 1
```

Route Reflector

The configurations in this section apply to BGP Route Reflectors (RR).

Reduce the iBGP Mesh Inside an Autonomous System

Use Route Reflectors to reduce the iBGP mesh inside an Autonomous System (AS).

Topology

In this example, R2, R5, and R4 would have to maintain a full mesh among themselves, but by making R5 the Route Reflector, R2 (Client1) has an iBGP session with the RR only, but not with R4 (Client 2). The routes learned from R2 are advertised to the other clients, and to iBGP peers outside the cluster; the iBGP routes learned from iBGP peers outside the cluster are advertised to R2. This reduces the iBGP peer connections in AS1.

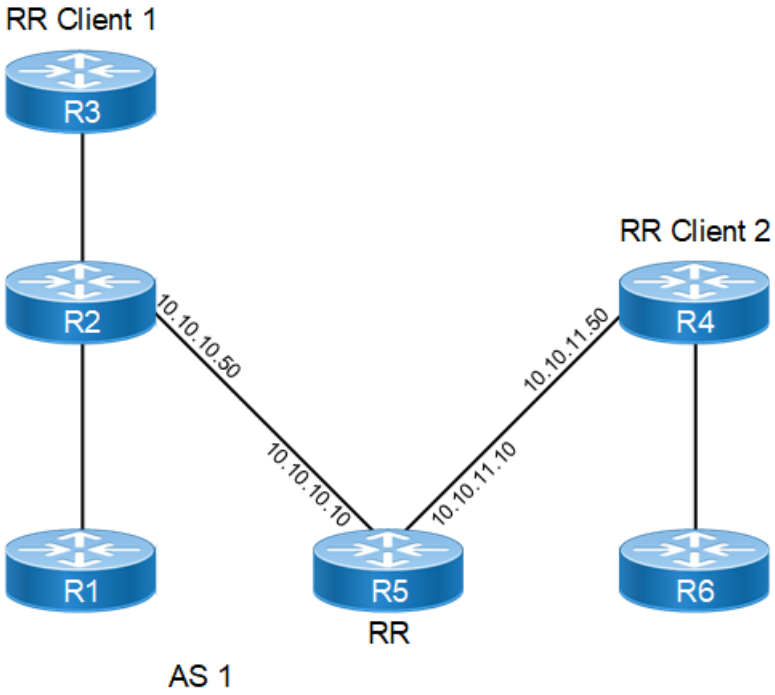


Figure 1-60: BGP Route Reflector

RR (R5)

`#configure terminal`	Enter configure mode.
`(config)#router bgp 1`	Define the routing process. The number `1` identifies the AS number of R5.
`(config-router)#neighbor 10.10.10.50 remote-as 1`	Define the BGP neighbor, and establish a TCP session. `10.10.10.50` is the IP address of one of the neighbors (R2), and `1` is the neighbor's AS number.
`(config-router)#neighbor 10.10.10.50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R2 as its client.
`(config-router)#neighbor 10.10.11.50 remote-as 1`	Define the BGP neighbor, and establish a TCP session. `10.10.11.50` is the IP address of one of the neighbors (R4), and `1` is the neighbor's AS number.
`(config-router)#neighbor 10.10.11.50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R4 as its client.
`(config-router)#exit`	Exit router mode.

RR Client 1 (R2)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remote-as 1`	Define the BGP neighbor, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R5), and `1` is the neighbor's AS number.
`(config-router)#exit`	Exit router mode.

RR Client 2 (R4)

`(config)#router bgp 1`	Define the routing process. The number `1` identifies the AS number of R4.
`(config-router)#neighbor 10.10.11.10 remote-as 1`	Define BGP neighbor, and establish a TCP session. `10.10.11.10` is the IP address of the neighbor (R5), and `1` is the neighbor's AS number.
`(config-router)#exit`	Exit router mode.

Validation

R5

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.50, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 10.12.4.152
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.10, Local port: 47983
Foreign host: 10.10.10.50, Foreign port: 179
Nexthop: 10.10.10.10
Nexthop global: fe80::a00:27ff:fe09:fd25
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 10.10.11.50, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.197
  local router ID 192.160.50.3
```

```
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.11.10, Local port: 39851
Foreign host: 10.10.11.50, Foreign port: 179
Nexthop: 10.10.11.10
Nexthop global: fe80::a00:27ff:fe52:45f6
Nexthop local: ::
BGP connection: non shared network
```

R3

```
#show ip bgp neighbors
BGP neighbor is 10.10.11.10, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:00:56
  Last read 00:00:56, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.11.50, Local port: 179
Foreign host: 10.10.11.10, Foreign port: 39851
Nexthop: 10.10.11.50
Nexthop global: fe80::a00:27ff:fe42:fb7a
Nexthop local: ::
BGP connection: non shared network
```

R2

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 1, local AS 1, internal link
```

```
  BGP version 4, local router ID 192.160.50.2, remote router ID 10.12.4.185
  BGP state = Established, up for 00:01:23
  Last read 00:01:23, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.50, Local port: 179
Foreign host: 10.10.10.10, Foreign port: 47983
Nexthop: 10.10.10.50
Nexthop global: fe80::a00:27ff:fe9c:f35d
Nexthop local: ::
BGP connection: non shared network
```

Multiple Route Reflectors

The basic rule of BGP is that a BGP speaker cannot advertise a route to an iBGP neighbor if that route was learned from another iBGP neighbor. Configuring a route reflector provides a means to circumvent this rule. The entire route reflector process is transparent to the clients, and no configuration is necessary on these clients.

Whenever an iBGP-speaking router receives a route update, it forwards the route to the neighbor without changing the nexthop IP address, thus making it an unreachable route, unless verified by an iGP (for example, neighbor x.x.x.x route-reflector-client).

- If a router is configured as a Route Reflector, it forwards the routes received by changing the nexthop address as itself, thus making the nexthop reachable.
- If a route is received from a client, the route is forwarded to the clients.
- If a route is received from a non-client, the route is forwarded to the clients and non-clients.

Topology

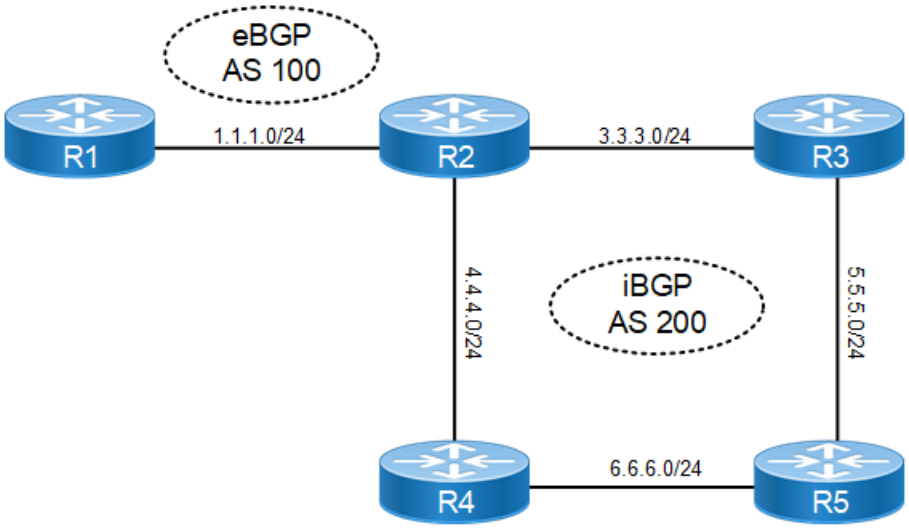


Figure 1-61: eBGP and iBGP Route Reflector Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip addr 1.1.1.1/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 100.100.100.100/32 secondary`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Define the eBGP neighbor (R2).
`(config-router)#network 100.100.100.100/32`	Advertise a route via eBGP connection to R2.
`(config-router)#exit`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 1.1.1.2/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 3.3.3.2/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth3`	Enter interface mode

(config-if)#ip address 4.4.4.2/24	Specify IP address for the interface.
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 1.1.1.1 remote-as 100	Define the eBGP neighbor (R1).
(config-router)#neighbor 4.4.4.1 remote-as 200	Define the iBGP neighbor (R4).
(config-router)#neighbor 3.3.3.1 remote-as 200	Define the iBGP neighbor (R3).
(config-router)#bgp cluster-id 4	Define a cluster ID (4) when multiple Route Reflectors exist.
(config-router)#neighbor 3.3.3.1 route-reflector-client	Configure R2 as the Route-Reflector and neighbor R3 as its client.
(config-router)#neighbor 4.4.4.1 route-reflector-client	Configure R2 as the Route-Reflector and neighbor R4 as its client.
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 3.3.3.1/24	Assign an IP address
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip addr 5.5.5.1/24	Assign an IP address
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 3.3.3.2 remote-as 200	Define the iBGP neighbor (R2).
(config-router)#neighbor 5.5.5.2 remote-as 200	Define the iBGP neighbor (R5).
(config-router)#neighbor 5.5.5.2 route-reflector-client	Configure R3 as the Route-Reflector and neighbor R5 as its client.
(config-router)#exit	Exit router mode.

R4

`#configure terminal`	Enter configure mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 6.6.6.1/24`	Specify an IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth4`	Enter interface mode
`(config-if)#ip address 4.4.4.1/24`	Specify an IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 4.4.4.2 remote-as 200`	Define the iBGP neighbor (R2).
`(config-router)#neighbor 6.6.6.2 remote-as 200`	Define the iBGP neighbor (R5).
`(config-router)#exit`	Exit router mode.

R5

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 5.5.5.2/24`	Specify an IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config-if)#interface eth2`	Enter interface mode
`(config-if)#ip address 6.6.6.2/24`	Specify an IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 5.5.5.1 remote-as 200`	Define the iBGP neighbor (R3).
`(config-router)#neighbor 6.6.6.1 remote-as 200`	Define the iBGP neighbor (R4).
`(config-router)#exit`	Exit router mode.

Validation

R2

```
#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 10.12.4.196, remote router ID 192.160.50.2
  BGP state = Established, up for 00:14:41
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 32 messages, 0 notifications, 0 in queue
  Sent 31 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 50649
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3.3.3.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 192.160.50.4
  BGP state = Established, up for 00:04:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 10 messages, 0 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 3, Offset 0, Mask 0x8
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.2, Local port: 179
Foreign host: 3.3.3.1, Foreign port: 32973
Nexthop: 3.3.3.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 4.4.4.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 192.160.50.6
  BGP state = Established, up for 00:00:16
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
```

```
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.2, Local port: 179
Foreign host: 4.4.4.1, Foreign port: 60398
Nexthop: 4.4.4.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:16:10
C     3.3.3.0/24 is directly connected, eth2, 00:15:59
C     4.4.4.0/24 is directly connected, eth3, 00:15:49
B     100.100.100.100/32 [20/0] via 1.1.1.1, eth1, 00:14:53
C     127.0.0.0/8 is directly connected, lo, 00:32:26
C     192.160.50.0/24 is directly connected, eth0, 00:32:22

Gateway of last resort is not set


#show ip bgp
BGP table version is 2, local router ID is 192.160.50.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.100/32
                      1.1.1.1              0         100           0       100
i

Total number of prefixes 1
Total number of neighbors 3
```

R1

```
#show bgp neighbors
BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 10.12.4.142, remote router ID 10.12.4.196
  BGP state = Established, up for 00:16:11
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
```

```
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 36 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 50649
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp summary
BGP router identifier 192.160.50.2, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
1.1.1.2                  4   200   34         36       1      0      0
00:16:18              0

Total number of neighbors 1

Total number of Established sessions 1
#
```

R3

```
#show ip bgp
BGP table version is 1, local router ID is 192.160.50.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.100.100.100/32
                      1.1.1.1              0         100           0       100
i

Total number of prefixes 1
#

#show ip bgp neighbors
BGP neighbor is 3.3.3.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 192.160.50.3
  BGP state = Established, up for 00:06:15
```

```
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 15 messages, 0 notifications, 0 in queue
  Sent 14 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 32973
Foreign host: 3.3.3.2, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 5.5.5.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 192.160.50.5
  BGP state = Established, up for 00:03:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 9 messages, 0 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.1, Local port: 179
Foreign host: 5.5.5.2, Foreign port: 39271
Nexthop: 5.5.5.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#

#show ip bgp summary
BGP router identifier 192.160.50.4, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                  V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
3.3.3.2                   4   200   15         14       1      0      0
00:06:26              1
5.5.5.2                   4   200    9         10       1      0      0
00:03:46              0

Total number of neighbors 2
```

R4

```
#show ip bgp
BGP table version is 1, local router ID is 192.160.50.6
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.100.100.100/32
                      1.1.1.1              0         100           0       100
i

Total number of prefixes 1
#

#sh ip bgp neighbors
BGP neighbor is 4.4.4.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.6, remote router ID 192.160.50.3
  BGP state = Established, up for 00:03:58
  Last read 00:00:28, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 10 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 60398
Foreign host: 4.4.4.2, Foreign port: 179
Nexthop: 4.4.4.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.6, remote router ID 192.160.50.5
  BGP state = Established, up for 00:03:52
```

```
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 9 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.1, Local port: 48257
Foreign host: 6.6.6.2, Foreign port: 179
Nexthop: 6.6.6.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#


#show ip bgp summary
BGP router identifier 192.160.50.6, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
4.4.4.2                   4   200   11         10       1      0      0
00:04:09              1
6.6.6.2                   4   200   10         10       1      0      0
00:04:03              0

Total number of neighbors 2

Total number of Established sessions 2
```

R5

```
#show ip bgp neighbors
BGP neighbor is 5.5.5.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.5, remote router ID 192.160.50.4
  BGP state = Established, up for 00:09:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 20 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
```

```
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.2, Local port: 39271
Foreign host: 5.5.5.1, Foreign port: 179
Nexthop: 5.5.5.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.5, remote router ID 192.160.50.6
  BGP state = Established, up for 00:07:36
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.2, Local port: 179
Foreign host: 6.6.6.1, Foreign port: 48257
Nexthop: 6.6.6.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
#

#sh ip bgp summary
BGP router identifier 192.160.50.5, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
5.5.5.1                  4   200   20         20       1      0      0
00:09:20              0
6.6.6.1                  4   200   17         18       1      0      0
00:07:52              0

Total number of neighbors 2
```

```
    Total number of Established sessions 2
    #
```

BGP Confederations

In BGP, nodes running iBGP protocols must be interconnected forming a full mesh. Confederation solves the iBGP full-mesh network complexity and inefficiency by splitting a large autonomous system domain into smaller autonomous system domains, called member autonomous systems. Member autonomous systems can form eBGP connections among themselves, to prevent full-mesh connections among each iBGP-running node.

The `bgp confederation identifier` command tells the router that it is a member of a confederation and the confederation ID. The `bgp confederation peers` command lists the member AS to which the router is connected.

In the following example, R1, R2, and R3 are members of the same confederation with different AS numbers.

Topology

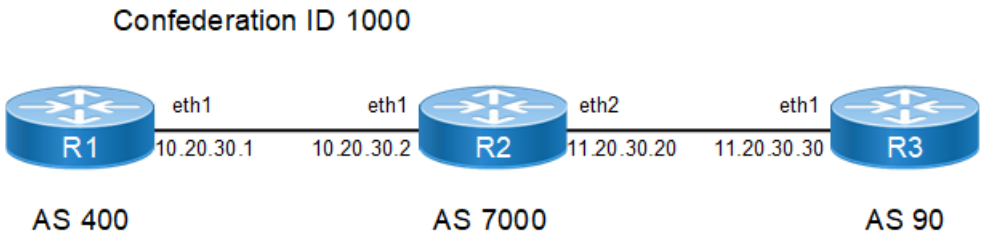


Figure 1-62: BGP Confederation

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID, the externally visible autonomous system number that identifies the BGP confederation as a whole.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).
`(config-router)#end`	Exit router and configure mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400 90`	Specify the neighbor ASN values for confederation membership.

`#configure terminal`	Enter configure mode.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).
`(config-router)#end`	Exit router and configure mode

R3

`#configure terminal`	Enter configure mode.
`(config-router)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 11.20.30.20 remote-as 7000`	Specify the neighbor's IP address (`11.20.30.20`) and the ASN value of the neighbor (`7000`).
`(config-router)#end`	Exit router and configure mode

Validation

R2

```
#sh ip bgp summary
BGP router identifier 192.168.52.3, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400    5          5       1      0      0
00:01:36              0
11.20.30.30              4    90    2          3       1      0      0
00:00:24              0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  Neighbor under common administration
  BGP state = Established, up for 00:01:25
  Last read 00:01:25, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35108
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 7000, external link
  BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:00:13
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33465
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
```

R1

```
#show ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:01:51
  Last read 00:01:51, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
```

```
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35108
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network


#sh ip bgp summary
BGP router identifier 192.168.52.3, local AS number 400
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4  7000    5          6       3      0      0
00:01:57              0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#sh ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 7000, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:00:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
```

```
Local host: 11.20.30.30, Local port: 33465
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4  7000    3          3       1      0      0
00:00:55              0

Total number of neighbors 1

Total number of Established sessions 1
```

Multiple Autonomous Systems

In the following example, R1 and R2 are members of the same confederation with the same AS numbers, and R3 is a member of the same confederation with a different AS number.

Topology

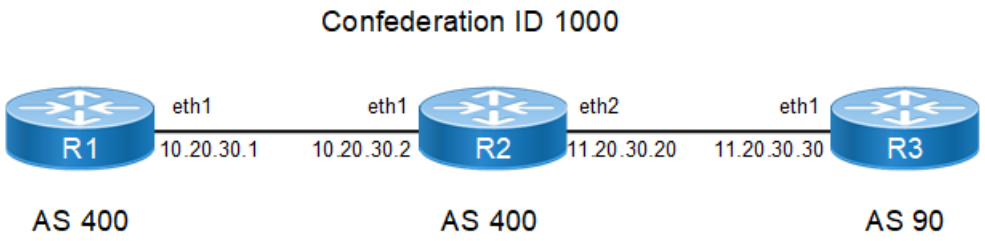


Figure 1-63: BGP Confederation with Multiple AS

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#neighbor 10.20.30.2 remote-as 400`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`400`).

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 90`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 11.20.30.20 remote-as 400`	Specify the neighbor's IP address (`11.20.30.20`) and the ASN value of the neighbor (`400`).

Validation

R2

```
#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 400
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400   16         16       1      0      0
00:07:27              0
11.20.30.30              4    90   32         42       1      0      0
00:00:27              0

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 400, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:08:10
  Last read 00:08:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 18 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35214
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 400, external link
  BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 14 notifications, 0 in queue
  Sent 42 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33623
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:36, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#show ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 400, local AS 400, internal link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:08:41
  Last read 00:08:41, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 35 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 16, neighbor version 16
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35214
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:09:03, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400
BGP table version is 16
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4   400   34         38      16      0      0
00:08:44              0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#show ip bgp summary
BGP router identifier 192.168.52.5, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4   400    2          2       1      0      0
00:00:15              0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 400, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
```

```
  Neighbor under common administration
  BGP state = Established, up for 00:02:24
  Last read 00:02:24, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.30, Local port: 33623
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
```

Outside Autonomous System

In the following example, R1 and R2 are members of the same confederation with different AS numbers, and R3 is a member outside the confederation.

Topology

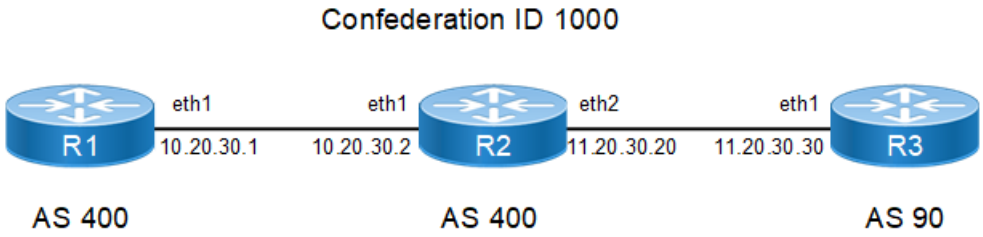


Figure 1-64: Single Confederation with Outside AS

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#neighbor 11.20.30.20 remote-as 1000`	Specify the neighbor's IP address (`11.20.30.20`) and the BGP confederation ID (`1000`).

Validation

R3

```
#show ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 1000, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 112 messages, 1 notifications, 0 in queue
  Sent 142 messages, 88 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 11.20.30.30, Local port: 33951
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:26, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

```
#sh ip bgp summary
BGP router identifier 192.168.52.5, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4  1000  113        230       1      0      0
00:01:13              0

Total number of neighbors 1

Total number of Established sessions 1
```

R2

```
#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400   22         22       1      0      0
00:10:04              0
11.20.30.30              4    90  179        202       1      0      0
00:00:42              0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:11:06
  Last read 00:11:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 24 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35444
```

```
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 1000, external link
  BGP version 4, remote router ID 192.168.56.103
  BGP state = Established, up for 00:01:44
  Last read 00:01:44, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 93 messages, 88 notifications, 0 in queue
  Sent 204 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33951
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:02:00, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#sh ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400
BGP table version is 34
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4  7000   77         91      34      0      0
00:10:18              0

Total number of neighbors 1

Total number of Established sessions 1
#sh ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:11:40
  Last read 00:11:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 80 messages, 0 notifications, 0 in queue
  Sent 82 messages, 12 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 35, neighbor version 35
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 3; dropped 2
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35444
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:12:47, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

BGP Authentication

BGP authentication allows users to receive selected routing information, enhancing security of their network traffic. When BGP authentication is enabled on a router, the router verifies routing packets it receives by exchanging a password that is configured on both the sending and receiving routers.

In this example, both R1 and R2 have ABC as the password. Configure the same password on all routers that are to communicate using BGP in a network.

Topology

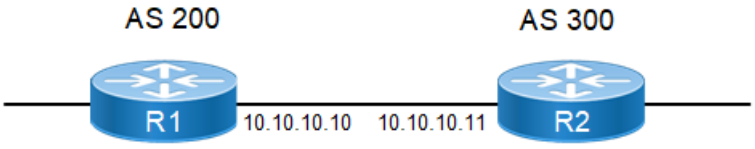


Figure 1-65: BGP Authentication

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remote-as 300`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `300` is the neighbor's AS number.
`(config-router)#neighbor 1.1.1.1 authentication-key 0 ABC`	Specify the key.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 300`	Define the routing process. The number `300` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.
`(config-router)#neighbor 1.1.1.1 authentication-key 0 ABC`	Specify the key.

Validation

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:09:18
  Last read 00:09:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 20 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.11, Local port: 53545
Foreign host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
```

Dynamic BGP Peering

BGP Dynamic Neighbors is a quick way of setting up BGP on device like a Hub router where user is expecting numerous BGP neighbors. Before dynamic neighbors, user had to provide a large amount of configuration to work with all these neighbors. This new feature dramatically reduces the amount and complexity of CLI configuration on the router and save CPU and memory usage.

BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. Each range can be configured as a subnet IP address. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups.

After a subnet range is configured for a BGP peer group and a TCP session is initiated by another router for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. After the initial

configuration of subnet ranges and activation of the peer group, dynamic BGP neighbor creation does not require any further CLI configuration on the initial router. Other routers can establish a BGP session with the initial router, but the initial router need not establish a BGP session to other routers if the IP address of the remote peer used for the BGP session is not within the configured range.

A dynamic BGP neighbor will inherit any configuration for the peer group. In larger BGP networks, implementing BGP dynamic neighbors can reduce the amount and complexity of CLI configuration and save CPU and memory usage. Both IPv4 and IPV6 peering is supported.

IPv4 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

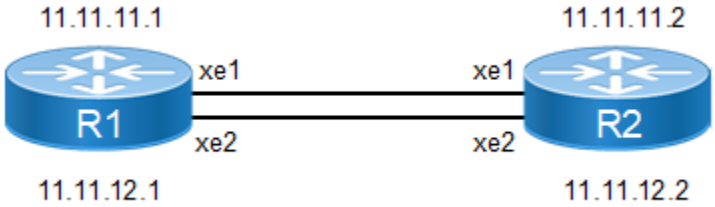


Figure 1-66: IPv4 IBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ip add 11.11.12.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16`	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16
`(config-router)#neighbor IPV4_IBGP_PEER remote-as 100`	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.

#configure terminal	Enter configure mode.
(config-router)#network 33.33.33.33/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode for loopback.
(config-if)#ip address 22.22.22.22/32 secondary	Assign a secondary IP address.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor 11.11.11.1 remote-as 100	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
(config-router)#neighbor 11.11.12.1 remote-as 100	Create a static BGP neighbor 11.11.12.1 in remote AS 100.
(config-router)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
#show ip bgp summary

BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.2              4   100   42         43       2      0      0
00:20:25              1
*11.11.12.2              4   100   42         43       2      0      0
00:20:25              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_IBGP_PEER
  listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)
```

```
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2
Total number of Established sessions 2


#show ip bgp neighbors

BGP neighbor is 11.11.11.2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.1, Local port: 40361
Foreign host: 11.11.11.2, Foreign port: 179
Nexthop: 11.11.11.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
```

```
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.1, Local port: 33478
Foreign host: 11.11.12.2, Foreign port: 179
Nexthop: 11.11.12.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show running-config bgp

router bgp 100
 bgp router-id 1.1.1.1
 network 33.33.33.33/32
 neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16
 neighbor IPV4_IBGP_PEER remote-as 100


#show ip bgp
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  22.22.22.22/32   11.11.11.2            0         100           0        i
* i                   11.11.12.2            0         100           0        i
*>   33.33.33.33/32   0.0.0.0               0         100          32768    i

Total number of prefixes 2
```

R2

```
#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.11.11.1               4   100   55         56       3      0      0
00:26:21              1
11.11.12.1               4   100   55         56       3      0      0
00:26:21              1

Total number of neighbors 2
Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.2, Local port: 179
Foreign host: 11.11.11.1, Foreign port: 40361
Nexthop: 11.11.11.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.2, Local port: 179
Foreign host: 11.11.12.1, Foreign port: 33478
Nexthop: 11.11.12.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   22.22.22.22/32   0.0.0.0              0         100           32768    i
```

```
*>i  33.33.33.33/32   11.11.11.1          0          100          0        i
* i                   11.11.12.1          0          100          0        i

Total number of prefixes 2
```

IPv4 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with vrf enabled on the device and interface being part of vrf. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

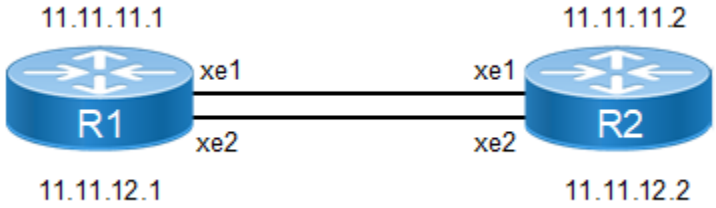


Figure 1-67: IPv4 VRF IBGP Peering

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrfA`	Create a VRF, vrfA on the router.
`(config-vrf)#rd 1:1`	Assign a route distinguisher to VRF.
`(config-if)#exit`	Exit VRF mode and return to Configure mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip add 11.11.12.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#address-family ipv4 vrf vrfA`	Enter IPv4 VRF Address Family.
`(config-router)#neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16`	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16.
`(config-router)#neighbor IPV4_IBGP_PEER remote-as 100`	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.
`(config-router)#network 33.33.33.33/32`	Advertise the loopback network into BGP
`(config-router)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrfA`	Create a VRF, vrfA on router.
`(config-vrf)#rd 2:1`	Assign a route distinguisher to VRF.
`(config-if)#exit`	Exit VRF mode and return to Configure mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip address 11.11.11.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip add 11.11.12.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#address-family ipv4 vrf vrfA`	Enter IPv4 VRF Address Family.
`(config-router)#neighbor 11.11.11.1 remote-as 100`	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
`(config-router)#neighbor 11.11.12.1 remote-as 100`	Create a static BGP neighbor 11.11.12.1 in remote AS 100
`(config-router)#network 22.22.22.22/32`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

Validation

R1

```
#show running-config bgp
!
router bgp 100
 bgp router-id 1.1.1.1
 !
 address-family ipv4 vrf vrfA
 neighbor IPV4_VRF_IBGP_PEER peer-group range 11.11.0.0/16
 neighbor IPV4_VRF_IBGP_PEER remote-as 100
 neighbor IPV4_VRF_IBGP_PEER activate
 neighbor IPV4_VRF_IBGP_PEER send-community extended
 exit-address-family
!

#show ip bgp summary vrf vrfA
BGP router identifier 11.11.11.1, local AS number 100
BGP VRF vrfA Route Distinguisher: 1:1
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.2              4   100    3          3       1      0      0
00:01:00              0
*11.11.12.2              4   100    3          3       1      0      0
00:00:55              0
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_IBGP_PEER
  listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2

Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 11.11.11.1, remote router ID 11.11.11.2
  BGP state = Established, up for 00:07:26
  Last read 00:00:26, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.1, Local port: 36365
Foreign host: 11.11.11.2, Foreign port: 179
Nexthop: 11.11.11.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 11.11.11.1, remote router ID 11.11.11.2
  BGP state = Established, up for 00:07:21
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.1, Local port: 38144
Foreign host: 11.11.12.2, Foreign port: 179
Nexthop: 11.11.12.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

IPv4 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

Figure 1-68: IPv4 EBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor 11.11.11.2 remote-as 200`	Create a static neighbor 11.11.11.2 with remote AS 200.

`#configure terminal`	Enter configure mode.
`(config-router)#network 33.33.33.33/32`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 22.22.22.22/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ip address 11.11.11.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ip add 11.11.12.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16`	Create a dynamic peer-group, IPV4_EBGP_PEER.
`(config-router)#neighbor IPV4_EBGP_PEER remote-as 100`	Assign remote AS with the peer-group IPV4_EBGP_PEER.
`(config-router)#neighbor IPV4_EBGP_PEER optional-as 300`	Assign optional AS with the peer-group IPV4_EBGP_PEER
`(config-router)#network 22.22.22.22/32`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 44.44.44.44/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ip add 11.11.12.3/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 300`	Enter Router BGP mode.
`(config-router)#bgp router-id 3.3.3.3`	Assign a BGP router ID.
`(config-router)#neighbor 11.11.12.2 remote-as 200`	Create a static BGP neighbor 11.11.12.2 with remote AS 200.

#configure terminal	Enter configure mode.
(config-router)#network 44.44.44.44/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R2

```
#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.1              4   100   29         29       3      0      0
00:13:10              1
*11.11.12.3              4   300   27         27       3      0      0
00:12:20              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_EBGP_PEER
  listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2

#show running-config bgp
!
router bgp 200
 bgp router-id 2.2.2.2
 network 22.22.22.22/32
 neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16
 neighbor IPV4_EBGP_PEER remote-as 100
 neighbor IPV4_EBGP_PEER optional-as 300


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 200, external link
 Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:17:15
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 37 messages, 0 notifications, 0 in queue
  Sent 38 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
```

```
  IPV4_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.2, Local port: 42252
Foreign host: 11.11.11.1, Foreign port: 179
Nexthop: 11.11.11.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.3, remote AS 300, local AS 200, external link
 Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:13:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 29 messages, 0 notifications, 0 in queue
  Sent 30 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  IPV4_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.2, Local port: 59839
Foreign host: 11.11.12.3, Foreign port: 179
Nexthop: 11.11.12.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

IPv6 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1/64 and 11:11:12::1/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

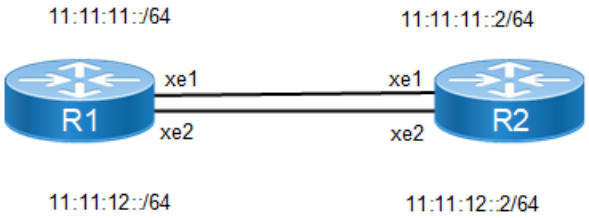


Figure 1-69: IPv6 IBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 33::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ipv6 address 11:11:12::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor IPV6_IBGP_PEER peer-group range 11:11::/16`	Create a dynamic peer-group, IPV6_IBGP_PEER with a dynamic range 11:11::/16
`(config-router)#neighbor IPV6_IBGP_PEER remote-as 100`	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
`(config-router)#neighbor IPV6_IBGP_PEER limit 1`	Set peer group neighbors limit to 1. Only one BGP session will be up.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#neighbor IPV6_IBGP_PEER activate`	Activate the peer group, IPV6_IBGP_PEER in the IPv6 address family.
`(config-router-af)#network 33::1/128`	Advertise the loopback network into the BGP IPv6 address family.
`(config-router-af)#end`	Exit from Router BGP address family mode.

R2

`#Configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 22::2/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.

(config-if)#ipv6 address 11:11:11::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)#ipv6 address 11:11:12::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor 11:11:11::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#neighbor 11:11:12::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#address-family ipv6 unicast	Enter the IPv6 Unicast Address Family.
(config-router-af)#network 22::2/128	Advertise the loopback network into BGP.
(config-router-af)#neighbor 11:11:12::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#neighbor 11:11:11::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#end	Exit from Router BGP address family mode.

Validation

R1

```
#show ipv6 bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::2             4   100    6          6       2      0      0
00:01:41              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_IBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 1/(1)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp peer-group IPV6_IBGP_PEER

BGP dynamic peer-group is IPV6_IBGP_PEER, IBGP, remote AS 100
```

```
  BGP dynamic peer-group IPV6_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *11:11:11::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
For address family: IPv6 Unicast
  Peer-group member:
  *11:11:11::2
  Index 0, Offset 0, Mask 0x0
  1 accepted prefixes, 1 announced prefixes


#show bgp ipv6
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  22::2/128        11:11:11::2(fe80::5054:ff:fe95:85ec)
                                          0         100           0        i
*>   33::1/128        ::                   0         100           32768    i

Total number of prefixes 2

#show running-config bgp
!
router bgp 100
 bgp router-id 1.1.1.1
 neighbor IPV6_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_IBGP_PEER remote-as 100
 neighbor IPV6_IBGP_PEER limit 1
 !
 address-family ipv6 unicast
 network 33::1/128
 neighbor IPV6_IBGP_PEER activate
 exit-address-family


#show bgp neighbors
BGP neighbor is 11:11:11::2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV6_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:04:17
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
 Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1
 Index 0, Offset 0, Mask 0x1
 IPV6_IBGP_PEER peer-group member
 Community attribute sent to this neighbor (both)
 0 accepted prefixes
 0 announced prefixes

For address family: IPv6 Unicast
 BGP table version 2, neighbor version 2
 Index 0, Offset 0, Mask 0x0
 IPV6_IBGP_PEER peer-group member
 Community attribute sent to this neighbor (both)
 1 accepted prefixes
 1 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:11::1, Local port: 42410
Foreign host: 11:11:11::2, Foreign port: 179
Nexthop: 1.1.1.1
Nexthop global: 11:11:11::1
Nexthop local: fe80::5054:ff:fe51:f74
BGP connection: shared network
```

IPV6 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with VRF enabled on the device and interface being part of VRF. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1 and 11:11:12::1. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

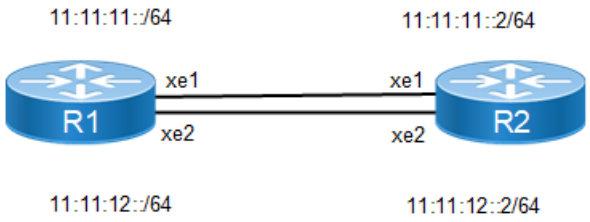


Figure 1-70: IPv6 VRF IBGP peering

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrfA`	Configure a VRF, vrfA.
`(config-vrf)#rd 1:1`	Configure a route distinguisher to VRF.
`(config-vrf)#router-id 7.7.7.7`	Configure a router ID.
`(config-vrf)#exit`	Exit from VRF mode and return to Configuration mode.

(config)#interface xe1	Enter interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:11::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:12::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#address-family ipv6 vrf vrfA	Enter IPv6 VRF Address Family.
(config-router-af)#neighbor IPV6_VRF_IBGP_PEER peer-group range 11:11::1/16	Configure a dynamic peer group, IPV6_IBGP_PEER with a dynamic range value.
(config-router-af)#neighbor IPV6_VRF_IBGP_PEER remote-as 100	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter configure mode.
(config)#ip vrf vrfA	Configure a VRF, vrfA.
(config-vrf)#rd 2:1	Configure a route distinguisher to VRF.
(config-vrf)#router-id 1.1.1.1	Configure a router ID.
(config-vrf)#exit	Exit from VRF mode and return to Configuration mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:11::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to vrf.
(config-if)#ipv6 address 11:11:12::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)#address-family ipv6 vrf vrfA	Enter IPv6 VRF Address Family.
(config-router-af)#neighbor 11:11:12::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router-af)#neighbor 11:11:11::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
#show ipv6 bgp summary vrf vrfA
BGP router identifier 7.7.7.7, local AS number 100
BGP VRF vrfA Route Distinguisher: 1:1
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::2             4   100    6          6       1      0      0
00:00:17              0
*11:11:12::2             4   100    7         10       1      0      0
00:00:15              0
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_VRF_IBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1

Total number of neighbors 2

Total number of Established sessions 2


#show running-config bgp
!
router bgp 100
 !
 address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_VRF_IBGP_PEER remote-as 100
 neighbor IPV6_VRF_IBGP_PEER activate
 neighbor IPV6_VRF_IBGP_PEER send-community extended
 exit-address-family
!

#show ip bgp peer-group vrf vrfA

BGP dynamic peer-group is IPV6_VRF_IBGP_PEER, IBGP, remote AS 100
  BGP dynamic peer-group IPV6_VRF_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv6 Unicast
  Peer-group member:
  *11:11:12::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
  Peer-group member:
```

```
  *11:11:11::2
  Index 2, Offset 0, Mask 0x4
  0 accepted prefixes, 0 announced prefixes

#show running-config bgp
!
router bgp 100
 !
 address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_VRF_IBGP_PEER remote-as 100
 neighbor IPV6_VRF_IBGP_PEER activate
 neighbor IPV6_VRF_IBGP_PEER send-community extended
 exit-address-family
!
#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:13
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 2 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  IPV6_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:11::1, Local port: 179
Foreign host: 11:11:11::2, Foreign port: 48206
Nexthop: 7.7.7.7
Nexthop global: 11:11:11::1
Nexthop local: fe80::5054:ff:fe51:f74
BGP connection: shared network
Last Reset: 00:02:18, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)

BGP neighbor is 11:11:12::2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:11
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 3 notifications, 0 in queue
```



```
  Sent 13 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  IPV6_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:12::1, Local port: 179
Foreign host: 11:11:12::2, Foreign port: 49010
Nexthop: 7.7.7.7
Nexthop global: 11:11:12::1
Nexthop local: fe80::5054:ff:fe8b:8f5c
BGP connection: shared network
Last Reset: 00:02:16, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)
```

IPv6 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11:11:11::/64 and 11:11:12::/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

Figure 1-71: IPv6 EBGP peering

R1

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 33::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:11::2 remote-as 200`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.

`(config-router-af)#neighbor 11:11:11::2 activate`	Activate the neighbor in the address family.
`(config-router-af)#network 33::1/128`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 22::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1
`(config-if)#ipv6 address 11:11:11::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ipv6 address 11:11:12::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#neighbor IPV6_EBGP_PEER peer-group range 11::1/16`	Configure a dynamic peer group, IPV6_EBGP_PEER.
`(config-router)#neighbor IPV6_EBGP_PEER remote-as 100`	Configure remote AS with peer group, IPV6_EBGP_PEER.
`(config-router)#neighbor IPV6_EBGP_PEER optional-as 300`	Configure optional AS with peer group, IPV6_EBGP_PEER.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Unicast Address Family.
`(config-router-af)#neighbor IPV6_EBGP_PEER activate`	Activate peer group in the address family.
`(config-router-af)#network 22::1/128`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

R3

`#Configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 44::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2
`(config-if)#ipv6 address 11:11:12::3/64`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 300`	Enter Router BGP mode.
`(config-router)#bgp router-id 3.3.3.3`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:12::2 remote-as 200`	Configure the BGP neighbor by specifying the neighbor IP address.

(config-router)#address-family ipv6 unicast	Enter the IPv6 Unicast Address Family.
(config-router-af)#neighbor 11:11:12::2 activate	Activate the neighbor in address family.
(config-router-af)#network 44::1/128	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R2

```
#show ipv6 bgp sum
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::1             4   100    9         11       5      0      0
00:01:28              1
*11:11:12::3             4   300    6          6       5      0      0
00:01:14              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_EBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2


#show running-config bgp
!
router bgp 200
 bgp router-id 2.2.2.2
 neighbor IPV6_EBGP_PEER peer-group range 11::/16
 neighbor IPV6_EBGP_PEER remote-as 100
 neighbor IPV6_EBGP_PEER optional-as 300
 !
 address-family ipv6 unicast
 network 22::1/128
 neighbor IPV6_EBGP_PEER activate
 exit-address-family
!

#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::1, remote AS 100, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:15
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 12 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
  Index 0, Offset 0, Mask 0x0
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
Local host: 11:11:11::2, Local port: 53043
Foreign host: 11:11:11::1, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: 11:11:11::2
Nexthop local: fe80::5054:ff:fe95:85ec
BGP connection: shared network
Last Reset: 00:02:20, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 11:11:12::3, remote AS 300, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:02:01
  Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
  Sent 8 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
```

```
  Index 0, Offset 0, Mask 0x0
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:12::2, Local port: 47743
Foreign host: 11:11:12::3, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: 11:11:12::2
Nexthop local: fe80::5054:ff:fee5:b088
BGP connection: shared network
```

VPNV4 Configuration

Below mentioned topology displays bgp vpnv4 configuration on PE nodes, R1 and R3. IBGP peering will be formed on the loopback interface of R1 and R3; also IGP is running between all the routers.

Topology

Figure 1-72: IPv4 IBGP VPNv4 Configuration

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrf1`	Create a VRF, vrf1.
`(config-vrf)#rd 100:1`	Configure a route distinguisher value.
`(config-vrf)#route-target export 100:1`	Configure a route target export value to VRF.
`(config-vrf)#route-target import 200:1`	Configure a route target import value to VRF.
`(config-vrf)#exit`	Exit from VRF configuration mode.
`(config)#router ldp`	Enter Router LDP mode.
`(config-router)#router-id 3.3.3.3`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode.
`(config)#interface xe5`	Enter Interface configuration mode.
`(config-if)#ip vrf forwarding vrf1`	Configure the interface to a VRF.
`(config-if)#ip address 1.1.1.1/24`	Assign an IP address to the interface.
`(config-if)#exit`	Exit from Interface configuration mode.
`(config-if)#interface xe1`	Enter another interface.
`(config-if)#ip address 11.11.11.1/24`	Assign an IP address to the interface.
`(config-if)#label-switching`	Enable label switching on interface.
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on interface.
`(config-if)#exit`	Exit from Interface configuration mode.

(config-if)#interface lo	Enter the loopback interface.
(config-if)#ip address 20.20.20.20/32 secondary	Assign a secondary IP address to the interface.
(config-if)#exit	Exit from Interface Configuration mode.
(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 11.11.11.0/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#network 20.20.20.20/32 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf1	Create an OSPF process on VRF.
(config-router)#network 1.1.1.1/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#redistribute bgp	Redistribute BGP into OSPF.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.
(config-router)#neighbor lo_peer peer-group range 30.30.30.30/32	Configure a dynamic peer group with the range command.
(config-router)#neighbor lo_peer remote-as 100	Configure remote AS to the peer group.
(config-router)#neighbor lo_peer update-source lo	Configure BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter the VPNv4 Address Family.
(config-router-af)#neighbor lo_peer activate	Activate the peer group in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf1	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 VRF address family.
(config-router)#end	Exit from the Router BGP mode.

R2

#Configure terminal	Enter Configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#router-id 4.4.4.4	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode.
(config-if)#interface xe2	Enter Interface Configuration mode.
(config-if)#ip address 12.12.12.2/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface xe1	Enter another Interface.
(config-if)#ip address 11.11.11.2/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.

(config-if)#exit	Exit from Interface mode.
(config)#router ospf 100	Create an OSPF process.
(config-router)#network 11.11.11.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#network 12.12.12.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#end	Exit from Router BGP mode.

R3

#Configure terminal	Enter Configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#router-id 5.5.5.5	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode.
(config)#ip vrf vrf2	Create a VRF, vrf2.
(config-vrf)#rd 200:1	Configure a route distinguisher value.
(config-vrf)#route-target export 200:1	Configure a route target export value to VRF.
(config-vrf)#route-target import 100:1	Configure a route target import value to VRF.
(config-vrf)#exit	Exit from VRF configuration mode.
(config)#interface xe1	Enter Interface configuration mode.
(config-if)#ip vrf forwarding vrf2	Configure an interface to a VRF.
(config-if)#ip address 2.2.2.3/24	Assign an IP address to the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface xe2	Enter another interface.
(config-if)#ip address 12.12.12.3/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface lo	Enter loopback interface.
(config-if)#ip address 30.30.30.30/32 se	Assign a secondary IP address to the interface.
(config-if)#exit	Exit from Interface mode.
(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 12.12.12.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#network 30.30.30.30/32 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf2	Create an OSPF process on VRF.
(config-router)#network 2.2.2.3/24 area 0	Define the interface on which OSPF runs, and associate the area ID.
(config-router)#redistribute bgp	Redistribute BGP into OSPF.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.

(config-router)#neighbor 20.20.20.20 remote-as 100	Configure BGP neighbor by specifying a neighbor IP address.
(config-router)#neighbor 20.20.20.20 update-slo	Define the BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family.
(config-router-af)#neighbor 20.20.20.20 act	Activate the neighbor in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf2	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 address family.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
#show running-config router bgp
router bgp 100
 neighbor lo_peer peer-group range 30.30.30.30/32
 neighbor lo_peer remote-as 100
 neighbor lo_peer update-source lo
 !
 address-family vpnv4 unicast
 neighbor lo_peer activate
 exit-address-family
 !
 address-family ipv4 vrf vrf1
 redistribute ospf 200
 exit-address-family
!

#show ip bgp vpnv4 all summary
BGP router identifier 192.168.52.3, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*30.30.30.30             4   100    4          4       2      0      0
00:00:37              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: lo_peer
  listen range:  30.30.30.30/32
  Total number of dynamically created neighbors/limit: 1/(200)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for VPNv4 Unicast address-
family: 1

Total number of neighbors 1

Total number of Established sessions 1
```

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:1 (Default for VRF vrf1)
*>   1.1.1.0/24       0.0.0.0               1         100           32768    ?
*>i  2.2.2.0/24       30.30.30.30           1         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 200:1
*>i  2.2.2.0/24       30.30.30.30           1         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1


#show ip bgp vpnv4 all 1.1.1.0
Route Distinguisher: 100:1
  Local
    20.20.20.20 (metric 12) from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid,
internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

Route Distinguisher: 200:1 (Default for VRF vrf2)
  Local
    20.20.20.20 from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid,
internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019


#show ip bgp peer-group

BGP dynamic peer-group is lo_peer, IBGP, remote AS 100
  BGP dynamic peer-group lo_peer listen range group members:
  30.30.30.30/32
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *30.30.30.30
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
For address family: VPNv4 Unicast
  Peer-group member:
  *30.30.30.30
  Index 0, Offset 0, Mask 0x0
  1 accepted prefixes, 1 announced prefixes
```

R2

```
R2#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:1 (Default for VRF vrf1)
*>   1.1.1.0/24       0.0.0.0              1         100           32768    ?
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 200:1
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1
R2#
```

R3

```
R3#show ip bgp vpnv4 all 1.1.1.0
Route Distinguisher: 100:1
  Local
    20.20.20.20 (metric 12) from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid, internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

Route Distinguisher: 200:1 (Default for VRF vrf2)
  Local
    20.20.20.20 from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid, internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

R3#
```

Enable eBGP Multihop

This example shows the minimum configuration required for enabling eBGP multihop on peers speaking BGP. eBGP multihop is used for routers that are not directly connected to each other. Typically, eBGP peers are directly connected, but if there is a requirement that necessitates this scenario, this configuration can be used.

Note: The IP addresses used in the configuration should be accessible through an IGP or static routing.

Topology

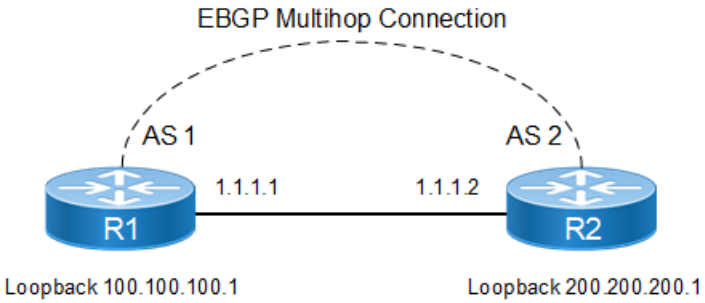


Figure 1-73: eBGP Multihop Connection

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 100.100.100.1/24 secondary`	Specify IP address to the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#ip route 200.200.200.0/24 1.1.1.2`	Specify route IP address.
`(config)#router bgp 1`	Define the routing process. The number 1 specifies the AS number of R1.
`(config-router)#neighbor 200.200.200.1 remote-as 2`	Define BGP neighbors, and establish a TCP session. 200.200.200.1 is the IP address of the neighbor (R2), and 2 is the neighbor's AS number.
`(config-router)#neighbor 200.200.200.1 update-source lo`	Define BGP neighbors, to update the source routes.
`(config-router)#neighbor 200.200.200.1 ebgp-multihop`	Define the neighbor `200.200.200.1` for eBGP multihops.
`(config-router)#end`	Exit BGP router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 200.200.200.1/24 secondary`	Specify IP address to the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#ip route 100.100.100.0/24 1.1.1.1`	Specify route IP address.
`(config)#router bgp 2`	Define the routing process. The number 2 specifies the AS number of R1.
`(config-router)#redistribute static`	Redistribute static route
`(config-router)#neighbor 100.100.100.1 remote-as 1`	Define BGP neighbors, and establish a TCP session. 100.100.100.1 is the IP address of the neighbor (R2), and 1 is the neighbor's AS number.

`(config-router)#neighbor 100.100.100.1 update-source lo`	Define BGP neighbors, to update the source routes.
`(config-router)#neighbor 100.100.100.1 ebgp-multihop`	Define the neighbor `100.100.100.1` for eBGP multihops.
`(config-router)#end`	Exit BGP router mode.

Validation

R1

```
#show ip bgp neighbors
BGP neighbor is 200.200.200.1, remote AS 2, local AS 1, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:00:22
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
  External BGP neighbor may be up to 255 hops away.
Local host: 100.100.100.1, Local port: 179
Foreign host: 200.200.200.1, Foreign port: 59458
Nexthop: 100.100.100.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp
BGP table version is 4, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.0/24 200.200.200.1        0         100           0       2 ?

Total number of prefixes 1
```

```
#show ip bgp neighbors
BGP neighbor is 200.200.200.1, remote AS 2, local AS 1, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:00:26
  Last read 00:00:26, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
  External BGP neighbor may be up to 255 hops away.
Local host: 100.100.100.1, Local port: 57260
Foreign host: 200.200.200.1, Foreign port: 179
Nexthop: 100.100.100.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:31, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)
```

R2

```
#sh ip bgp neighbors
BGP neighbor is 100.100.100.1, remote AS 1, local AS 2, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:00:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 1 notifications, 0 in queue
  Sent 7 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
```

```
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
  External BGP neighbor may be up to 255 hops away.
Local host: 200.200.200.1, Local port: 179
Foreign host: 100.100.100.1, Foreign port: 57260
Nexthop: 200.200.200.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:40, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)

#show ip bgp
BGP table version is 4, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.0/24 1.1.1.1             0         100           32768    ?

Total number of prefixes 1
```

Enable Peer Groups

A BGP speaker might have the same update policies for a set of its peers. This is very useful if you have to change the update policies for all of the peers: Changing individual routers for separate policies can be very time-consuming, thus, peer groups play an important role in creating and assigning policies to a group of routers.

BGP Peer Groups for Address-Family IPv4 Unicast

In the following scenario, R1, R2, and R3 belong to the same peer group ABC. R1, R2 and R3 are in AS 200 and R1 is the route reflector.R4 and R1 are eBGP peers .R4 is in AS 100.

Topology

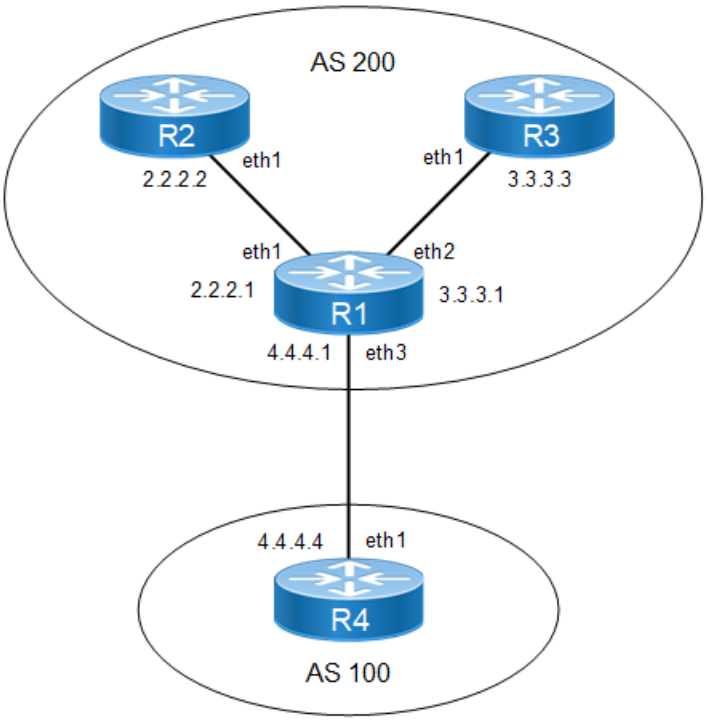


Figure 1-74: BGP Peer Groups with IPv4 Unicast Members

R1

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure IP address for Loopback interface
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure IP address for Loopback interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R1.
`(config-router)#neighbor ABC peer-group`	Create a peer group named ABC.
`(config-router)#neighbor ABC remote-as 200`	Assign options to the peer group named ABC.
`(config-router)#neighbor ABC route-reflector-client`	Configure the peer-group ABC to be route-reflector-client
`(config-router)#neighbor 2.2.2.2 peer-group`	
ABC	Define neighbor 2.2.2.2 (R2) as a peer group member.
`(config-router)#neighbor 3.3.3.3 peer-group`	
ABC	Define neighbor 3.3.3.3 (R3) as a peer group member.
`(config-router)#neighbor 4.4.4.4 remote-as`	
`100`	Define neighbor 4.4.4.4 (R4) is the IP address of R4 and 100 is the AS number.

`(config-router)#network 1.1.1.1/32`	Advertise the network 1.1.1.1/32
`(config-router)#network 11.11.11.11/32`	Advertise the network 11.11.11.11/32

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R2.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Create a TCP connection with neighbor `2.2.2.1` of AS `200`.

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R3.
`(config-router)#neighbor 3.3.3.1 remote-as 200`	Create a TCP connection with neighbor `3.3.3.1` of AS `200`.

R4

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Define the routing process. The number `100` specifies the AS number of R4.
`(config-router)#neighbor 4.4.4.1 remote-as 200`	Create a TCP connection with neighbor 4.4.4.1 of AS 200.

Validation

R1

```
R1#show ip bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 192.168.52.2, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 192.168.52.2, remote router ID 10.12.7.153
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 44280
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: fe80::a00:27ff:fe85:25d4
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 4.4.4.4, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 10.12.7.120
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 55493
```

```
Foreign host: 4.4.4.4, Foreign port: 179 Nexthop: 4.4.4.1
Nexthop global: fe80::a00:27ff:fe7e:674a
Nexthop local: ::
BGP connection: non shared network

R1#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
2.2.2.2                  4   200   12         12       1      0      0
00:05:02               0
3.3.3.3                  4   200   12         12       1      0      0
00:05:02               0
4.4.4.4                  4   100   12         12       1      0      0
00:05:02               0
Total number of neighbors 3
Total number of Established sessions 3
```

R2

```
R2#show ip bgp
BGP table version is 4, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       2.2.2.1               0         100           0        i
*>i  11.11.11.11/32   2.2.2.1               0         100           0        i

Total number of prefixes 2
R2#
```

R3

```
R3#show ip bgp
BGP table version is 8, local router ID is 10.12.65.121
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       3.3.3.1               0         100           0        i
*>i  11.11.11.11/32   3.3.3.1               0         100           0        i

Total number of prefixes 2
R3#
```

Peer-group can have either iBGP or eBGP peers but not both.

Validation

The configuration above fails with an appropriate error:

```
R1(config)#router bgp 200
R1(config-router)#neighbor 4.4.4.4 peer-group ABC
%% Peer with AS 100 cannot be in this peer-group, members must be all internal
or all external
R1(config-router)#
```

Peer group members inherit the properties of Outbound Policies configured for Peer-group.

R1

`#configure terminal`	Enter configure mode.
`(config)# ip access-list permit-1`	Configure access-list to permit 1.1.1.1/32
`(config-ip-acl)# permit any 1.1.1.1/32 any`	Configure a permit statement in the acl to permit 1.1.1.1/32
`(config-ip-acl)#exit`	Exit ip access-list mode
`(config)# route-map permit-only-1`	Configure route-map
`(config-route-map)# match ip address permit-1`	Configure a match statement in the route-map to match the access-list permit-1
`(config-route-map)#set local-preference 250`	
`(config-route-map)#exit`	
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R1.
`(config-router)# neighbor ABC route-map permit-only-1  out`	Configure the peer-group ABC with route-map in the outbound direction
`(config-router)#exit`	Exit router BGP mode
`(config# exit`	Exit configure terminal mode
`#clear ip bgp peer-group ABC soft out`	Do outbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

Validation

R1

```
R1#show bgp neighbors 2.2.2.2
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:07:01
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 28 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
```

```
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 2; dropped 1
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 42657
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:08:39, due to Hold Timer Expired (Notification sent)
Notification Error Message: (Hold Timer Expired/No sub-error code)

R1#show bgp neighbors 3.3.3.3
BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:11:46
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 29 messages, 0 notifications, 0 in queue
  Sent 32 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 179
Foreign host: 3.3.3.3, Foreign port: 48008
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

R2

```
R2#show ip bgp
BGP table version is 3, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       2.2.2.1               0         250           0        i
```

```
    Total number of prefixes 1
```

R3

```
    R3#show ip bgp
    BGP table version is 7, local router ID is 10.12.65.121
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal,
                  l - labeled, S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path
    *>i  1.1.1.1/32       3.3.3.1               0         250           0        i

    Total number of prefixes 1
```

Peer-group-members cannot be configured with Outbound Policies.

Validation

The above configuration fails with an appropriate error:

```
    R1(config)#router bgp 200
    R1(config-router)#neighbor 2.2.2.2 route-map permit-only-11 out
    %% Invalid command for a peer-group member
```

Peer-group-members inherit the properties of Inbound Policies configured for Peer-group.

R2

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.1/24`	Configure IP address for interface eth3
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter router bgp mode
`(config-router)#network 22.1.1.0/24`	Advertise the network of eth3 in BGP
`(config-router)#network 100.1.1.0/24`	Advertise the network of Loopback in BGP
`(config-router)#exit`	Exit router bgp mode

R3

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.2/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.2/24`	Configure IP address for interface eth3

(config-if)#exit	Exit interface mode
(config)#router bgp 200	Enter router bgp mode
(config-router)#network 22.1.1.0/24	Advertise the network of eth3 in BGP
(config-router)#network 100.1.1.0/24	Advertise the network of Loopback in BGP
(config-router)#exit	Exit router bgp mode

R1

#configure terminal	Enter configure mode.
(config)#ip access-list permit-22	Configure access-list to permit 22.1.1.0/24
(config-ip-acl)# permit any 22.1.1.0/24 any	Configure a permit statement to permit 22.1.1.0/24
(config-ip-acl)#exit	Exit ip access-list mode
(config)#route-map permit-only-22	Configure route-map
(config-route-map)#match ip address permit-22	Configure match statement in route-map to match the access-list permit-22
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Enter BGP router mode
(config-router)#neighbor ABC route-map permit-only-22 in	Configure the peer-group ABC with route-map in the inbound direction
(config-router)#exit	Exit router bgp mode
(config)# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC soft in	Do inbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

Validation

R1

```
R1#show ip bgp

BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, a add-path, g group-best, *
valid, > best, i - internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network             Next Hop             Metric        LocPrf
Weight  Path
*>   1.1.1.1/32         0.0.0.0              0             100          32768
i
*>   11.11.11.11/32     0.0.0.0              0             100          32768
i
*>i  22.1.1.0/24        2.2.2.2              0             100          0
i
* i                     3.3.3.3              0             100          0
i

Total number of prefixes 3
```

Peer group members can be configured with Inbound Policies

R1

#configure terminal	Enter configure mode.
(config)#ip access-list permit-100	Configure access-list to permit 100.1.1.0/24
(config-ip-acl)# permit any 100.1.1.0/24 any	Configure a permit statement to permit 100.1.1.0/24
(config-ip-acl)#exit	Exit ip access-list mode
(config)#route-map permit-only-100	Configure route-map
(config-route-map)#match ip address permit-100	Configure match statement in route-map to match the access-list permit-100
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Enter BGP router mode
(config-router)#neighbor 2.2.2.2 route-map permit-only-100 in	Configure the peer-group-member R2(2.2.2.2) with route-map in the inbound direction
(config-router)#exit	Exit router bgp mode
(config)# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC soft in	Do inbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

Validation

R1

```
R1#show ip bgp
BGP table version is 4, local router ID is 10.12.65.126
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.1/32       0.0.0.0               0         100           32768    i
*>   11.11.11.11/32   0.0.0.0               0         100           32768    i
*>i  22.1.1.0/24      3.3.3.3               0         100           0        i
*>i  100.1.1.0/24     2.2.2.2               0         100           0        i

Total number of prefixes 4
R1#
```

BGP Peer Groups for Address-Family IPv4 Labeled Unicast

Topology

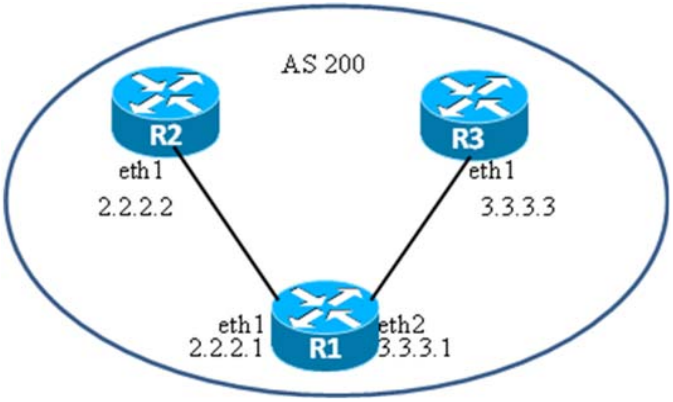


Figure 1-75: BGP Peer-Groups with IPv4 Labeled-Unicast Members

R1

`(config)# interface lo`	Enter interface mode for Loopback
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address for Loopback interface
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure ip address for Loopback interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R1.
`(config-router)#neighbor ABC peer-group`	Create a peer group named ABC.
`(config-router)#neighbor ABC remote-as 200`	Assign options to the peer group named ABC.
`(config-router)#neighbor 2.2.2.2 peer-group ABC`	Define neighbor 2.2.2.2 (R2) as a peer group member.
`(config-router)#neighbor 3.3.3.3 peer-group ABC`	Define neighbor 3.3.3.3 (R3) as a peer group member.
`(config-router)#address-family ipv4 labeled-unicast`	Enter address-family ipv4 labeled-unicast mode
`(config-router-af)#neighbor ABC activate`	Activate the peer-group ABC for address-family ipv4 labeled-unicast
`(config-router-af)#neighbor ABC route-reflector-client`	Configure the peer-group ABC to be route-reflector-client
`(config-router-af)# exit-address-family`	Exit address-family ipv4 labeled-unicast mode
`(config-router)#network 1.1.1.1/32`	Advertise the network 1.1.1.1/32
`(config-router)#network 11.11.11.11/32`	Advertise the network 11.11.11.11/32
`(config-router)#allocate-label all`	Allocate labels for all IPv4 prefixes advertised
`(config-router)#exit`	

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R2.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Create a TCP connection with neighbor 2.2.2.1 of AS 200.
`(config-router)#address-family ipv4 labeled-unicast`	Enter address-family ipv4 labeled-unicast mode
`(config-router-af)#neighbor 2.2.2.1 activate`	Activate the neighbor R1 for address-family ipv4 labeled-unicast
`(config-router-af)# exit-address-family`	Exit address-family ipv4 labeled-unicast mode
`(config-router)# exit`	Exit router bgp mode

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R3.
`(config-router)#neighbor 3.3.3.1 remote-as 200`	Create a TCP connection with neighbor 3.3.3.1 of AS 200.
`(config-router)#address-family ipv4 labeled-unicast`	Enter address-family ipv4 labeled-unicast mode
`(config-router-af)#neighbor 3.3.3.1 activate`	Activate the neighbor R1 for address-family ipv4 labeled-unicast
`(config-router-af)# exit-address-family`	Exit address-family ipv4 labeled-unicast mode
`(config-router)# exit`	Exit router bgp mode

Validation

R1

```
R1#show ip bgp labeled-unicast summary
BGP router identifier 10.12.65.126, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
2.2.2.2                  4   200   18         22       1      0      0
00:00:57               0
3.3.3.3                  4   200   18         20       1      0      0
00:00:01               0

Total number of neighbors 2

Total number of Established sessions 2
R1#


R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
```

```
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:01:05
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 16 messages, 2 notifications, 0 in queue
  Sent 20 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:10, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:00:09
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 16 messages, 2 notifications, 0 in queue
  Sent 20 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:19, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

R1#
```

R2

```
R2#show ip bgp
BGP table version is 3, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>il 1.1.1.1/32       2.2.2.1               0         100           0        i
* i                   2.2.2.1               0         100           0        i
*>il 11.11.11.11/32   2.2.2.1               0         100           0        i
* i                   2.2.2.1               0         100           0        i

Total number of prefixes 2
R2#




R2#show ip bgp 1.1.1.1/32
BGP routing table entry for 1.1.1.1/32
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, best, source
safi: 4
      Last update: Tue Aug 25 10:01:05 2020

  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
```

```
      Origin IGP, metric 0, localpref 100      valid, internal, source safi: 1
      Last update: Tue Aug 25 10:01:05 2020

R2#
R2#show ip bgp 11.11.11.11/32
BGP routing table entry for 11.11.11.11/32
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, best, source
safi: 4
      Last update: Tue Aug 25 10:01:05 2020

  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, source safi: 1
      Last update: Tue Aug 25 10:01:05 2020

R2#


R2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       2.2.2.1           -            24320
*>i 11.11.11.11/32   2.2.2.1           -            24321
R2#
```

R3

```
R3#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       3.3.3.1           -            24320
*>i 11.11.11.11/32   3.3.3.1           -            24321
R3#
```

Peer group members inherit the properties of Outbound Policies configured for Peer-group under Address-family ipv4 Labeled-Unicast

R1

`#configure terminal`	Enter configure mode.
`(config)# ip access-list permit-1`	Configure access-list to permit 1.1.1.1/32
`(config-ip-acl)# permit any 1.1.1.1/32 any`	Configure a permit statement in the acl to permit 1.1.1.1/32
`(config-ip-acl)#exit`	Exit ip access-list mode
`(config)# route-map permit-only-1`	Configure route-map

(config-route-map)# match ip address permit-1	Configure a match statement in the route-map to match the access-list permit-1
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R1.
(config-router)#address-family ipv4 labeled-unicast	Enter address-family ipv4 labeled-unicast mode
(config-router-af)# neighbor ABC route-map permit-only-1 out	Configure the peer-group ABC with route-map in the outbound direction
(config-router-af)#exit	Exit address-family mode
(config-router)#exit	Exit router bgp mode
(config# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC ipv4 labeled-unicast soft out	Do outbound soft reset for the peer-group ABC for the policy to take affect for the labelled-unicast peer-group members

Validation

R1

```
R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:14:24
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 46 messages, 2 notifications, 0 in queue
  Sent 53 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
```

```
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:14:29, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:13:28
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 47 messages, 2 notifications, 0 in queue
  Sent 53 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:13:38, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

R1#
```

R2

```
R2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
```

```
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       2.2.2.1           -            24320
R2#
```

R3

```
R3#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       3.3.3.1           -            24320
R3#
```

Peer-group-members inherit the properties of Inbound Policies configured for Peer-group under Address-family ipv4 Labeled-Unicast

Follow the configuration of R1,R2,R3 in the previous section with the following configuration

R2

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.1/24`	Configure IP address for interface eth3
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter router bgp mode
`(config-router)#network 22.1.1.0/24`	Advertise the network of eth3 in BGP
`(config-router)#network 100.1.1.0/24`	Advertise the network of Loopback in BGP
`(config-router)#allocate-label all`	Allocate labels for all IPv4 prefixes advertised
`(config-router)#exit`	Exit router bgp mode

R3

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.2/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.2/24`	Configure IP address for interface eth3
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter router bgp mode
`(config-router)#network 22.1.1.0/24`	Advertise the network of eth3 in BGP
`(config-router)#network 100.1.1.0/24`	Advertise the network of Loopback in BGP

(config-router)#allocate-label all	Allocate labels for all IPv4 prefixes advertised
(config-router)#exit	Exit router bgp mode

R1

#configure terminal	Enter configure mode.
(config)#ip access-list permit-22	Configure access-list to permit 22.1.1.0/24
(config-ip-acl)# permit any 22.1.1.0/24 any	Configure a permit statement to permit 22.1.1.0/24
(config-ip-acl)#exit	Exit ip access-list mode
(config)#route-map permit-only-22	Configure route-map
(config-route-map)#match ip address permit-22	Configure match statement in route-map to match the access-list permit-22
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Enter BGP router mode
(config-router)#address-family ipv4 labeled-unicast	Enter the address-family ipv4 labeled-unicast mode
(config-router-af)#neighbor ABC route-map permit-only-22 in	Configure the peer-group ABC with route-map in the inbound direction under address-family ipv4 labeled-unicast
(config-router-af)#exit-address-family	Exit address-family ipv4 labeled-unicast mode
(config-router)#exit	Exit router bgp mode
(config)# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC ipv4 labeled-unicast soft in	Do inbound soft reset for the peer-group ABC for the policy to take affect for the labelled-unicast peer-group members

Validation

R1

```
R1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>  1.1.1.1/32       0.0.0.0          24320          -
*>  11.11.11.11/32   0.0.0.0          24321          -
*>i 22.1.1.0/24      3.3.3.3          24322        24320
* i                  2.2.2.2           -            24320
*>i 100.1.1.0/24     3.3.3.3          24323          -
R1#


R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:45:38
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
```

```
  Received 123 messages, 2 notifications, 0 in queue
  Sent 126 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 14, neighbor version 14
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *permit-only-22
  Route map for outgoing advertisements is *permit-only-1
  1 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:45:43, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:44:42
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 124 messages, 2 notifications, 0 in queue
  Sent 127 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 14, neighbor version 14
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
```

```
  BGP table version 3, neighbor version 3
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *permit-only-22
  Route map for outgoing advertisements is *permit-only-1
  1 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:44:52, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

R1#
```

Route Redistribution in BGP

If there are routers that run both OSPF and BGP, certain OSPF routes might have to be sent to other eBGP peers. This can be achieved using the redistribution feature. Consider the following topology, in which R1 and R2 are eBGP peers, and R2 and R3 are OSPF peers. R2 is redistributing OSPF routes into BGP. The OSPF routes are sent to the R1 BGP routing table. This configuration assumes that all OSPF and eBGP sessions are up and running, and that only the redistribution must be configured.

Topology

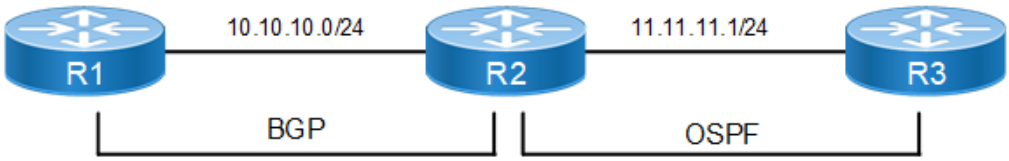


Figure 1-76: Redistribute with OSPF

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Define the routing process. The number `100` specifies the AS number of R2.
`(config-router)#redistribute ospf`	Redistribute OSPF routes in the R2 routing table into the R1 BGP routing table.
`(config-router)#exit`	Exit Router-BGP mode.

Validation

```
#show ip bgp
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   3.3.3.3/32       10.10.10.2            11        100            0       100
?
*>   11.11.11.0/24    10.10.10.2            1         100            0       100
?

Total number of prefixes 2
```

Add Multiple Instances of the Same Autonomous System

BGP supports adding the same AS number multiple times to influence the route selection process. This can be done using route maps, as described below.

Under normal circumstances, any route advertised by R1 is sent to R4 via two different routes, and then R4 selects the path from R2. This decision can be influenced by adding multiple instances of AS number 200 at R2.

Topology

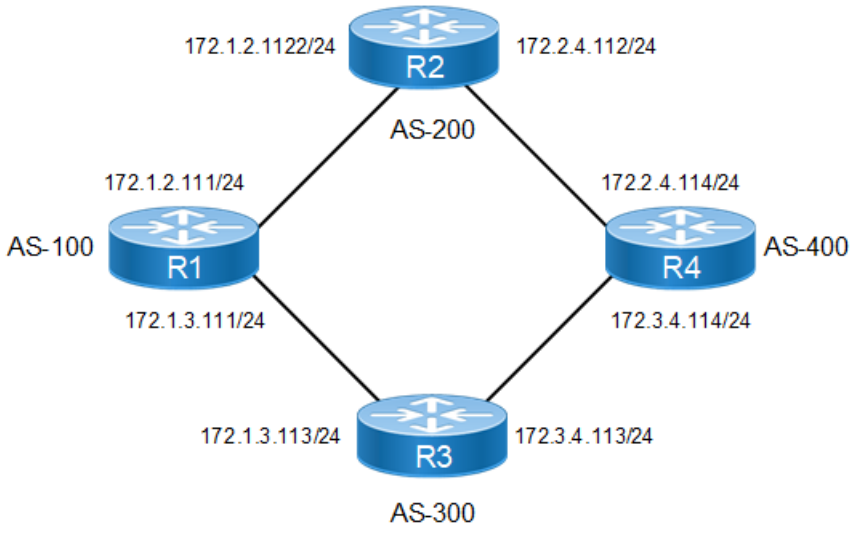


Figure 1-77: Multiple Instances of Same AS

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 44.44.44.1/24 secondary`	Specify the IP address for the interface.

`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 172.1.2.112 remote-as 200`	Define neighbor R2. `172.1.2.112` is the IP address of R2, and `200` is the AS number.
`(config-router)#neighbor 172.1.3.113 remote-as 300`	Define neighbor R3. `172.1.3.113` is the IP address of R2, and `300` is the AS number.
`(config-router)#network 44.44.44.0/24`	Advertise network `44.44.44.0/24` through BGP. This route reaches R4 via R2 and R3.

R2

`#configure terminal`	Enter configure mode.
`(config)#route-map mul_inst permit 10`	Define the route-map multiple instance with permit definition sequence number `10`.
`(config-route-map)#set as-path prepend 200 200`	Prepend AS number `200` two times to the AS_PATH attribute in the BGP Update message.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 172.1.2.111 remote-as 100`	Define neighbor R1. `172.1.2.111` is the IP address of R1, and `100` is the AS number.
`(config-router)#neighbor 172.2.4.114 remote-as 400`	Define neighbor R4. `172.2.4.114` is the IP address of R2, and `400` is the AS number.
`(config-router)#neighbor 172.2.4.114 route-map mul_inst out`	Apply route-map `multi_inst` to all outbound routes to R4.

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 300`	Define the routing process with AS number `300`.
`(config-router)#neighbor 172.1.3.111 remote-as 100`	Define neighbor R1. `172.1.3.111` is the IP address of R1, and `100` is the AS number.
`(config-router)#neighbor 172.3.4.114 remote-as 400`	Define neighbor R4. `172.3.4.114` is the IP address of R4, and `400` is the AS number.

R4

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Define the routing process with AS number `400`.
`(config-router)#neighbor 172.2.4.112 remote-as 200`	Define neighbor R2. `172.2.4.112` is the IP address of R2, and `200` is the AS number.
`(config-router)#neighbor 172.3.4.113 remote-as 300`	Define neighbor R3. `172.3.4.113` is the IP address of R3, and `300` is the AS number.

Validation

```
#show ip bgp
```

```
BGP table version is 1, local router ID is 44.44.44.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 44.44.44.0/24 0.0.0.0 0 100 32768 i

Total number of prefixes 1
```

Remove the Multi-Exit Disc Attribute from Update Messages

You can remove the Multi-Exit Disc (MED) attribute values from received update messages.

Topology

Figure 1-78: Remove MED Attribute

R1

`#configure terminal`	Enter configure mode.
`(config)#route-map med permit 1`	Define the route-map MED with permit definition sequence number `1`.
`(config-route-map)#set metric 400`	Set the metric value.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Define neighbor R2. `1.1.1.2` is the IP address of R2, and `200` is the AS number.
`(config-router)#neighbor 1.1.1.2 route-map med out`	Apply the route-map MED to all outbound routes to R2.
`(config)#interface xe2`	Enter interface mode
`(config-if)#ip ad 10.10.10.1/24`	Assign IP address
`(config-if)#no shutdown`	Make interface administratively up
`(config-if)#exit`	Exit interface mode
`(config)#ip route 100.0.0.0/8 10.10.10.2`	Configure the static route with the nexthop address.

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Define neighbor R2. `2.2.2.1` is the IP address of R2, and `200` is the AS number.

Removing Sent and Received MED values

The following describes how to remove the received and sent MED values, respectively.

R2 - Remove Received MED Value

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Define neighbor R1. `1.1.1.1` is the IP address of R1, and `100` is the AS number.
`(config-router)#neighbor 2.2.2.2 remote-as 200`	Define neighbor R3. `2.2.2.2` is the IP address of R3, and `200` is the AS number.
`(config-router)#bgp bestpath med remove-recv-med`	Enable the remove received MED value option.

R1 - Add Static Route

`(config)#router bgp 100`	Enter to router bgp mode
`(config-router)#redistribute static`	Redistribute the static routes

R2 - Remove Send MED Value

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Define neighbor R1. `1.1.1.1` is the IP address of R1, and `100` is the AS number.
`(config-router)#neighbor 2.2.2.2 remote-as 200`	Define neighbor R3. `2.2.2.2` is the IP address of R3, and `200` is the AS number.
`(config-router)#bgp bestpath med remove-send-med`	Enable the remove sent MED value option.

Validation

```
R2#show ip bgp
BGP table version is 2, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.0.0.0        1.1.1.1         removed     100           0       100 ?

Total number of prefixes 1


R3#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.0.0.0        1.1.1.1               400       100           0       100 ?

Total number of prefixes 1
```

BGP Four-Byte Autonomous System

Extended AS numbers can be mapped to 2-byte AS numbers if the value is less than, or equal to, 65535. If the AS number is higher than 65535, it cannot be mapped to a 2-byte AS number. Therefore, if a BGP speaker is configured with a non-mappable AS number, it must enable the BGP extended ASN capability in OcNOS.

Note: Autonomous System number 23456 is a reserved IANA number for AS transition; thus, it is recommended that no system be configured with 23456 as its AS number.

The extended ASN capability is disabled by default. However, when it is enabled, it is able to interoperate with a 2-byte AS-numbered speaker, in compliance with RFC 4893.

If a 4-byte AS number is configured in the provider's network using BGP MPLS VPN or standard IPv4/IPv6 BGP, it is recommended that the PE routers be 4-byte AS-enabled before connecting to 4-byte AS-enabled customer networks. For implications related to AS number transition issues, refer to RFC 4893.

You can also set up 4-byte AS-specific extended communities and route distinguishers (RDs) with limited capabilities. However, it is recommended that 2-byte AS-specific RDs and extended communities be used for regular deployment.

BGP encodes an ASN into four octets, so that more autonomous systems can be supported. Extended ASN capability is advertised in the Open message capabilities when the 4-octet ASN capability is enabled. When the 4-octet ASN capability is enabled, the valid ASN value range is <1-4294967295>, with the exception discussed in the first Note, above.

Note: Four-octet capability is disabled by default.

4-Octet ASN Capability Enabled on R1 and R2

In this example, 4-Octet ASN capability is enabled on BGP speakers R1 and R2.

Topology

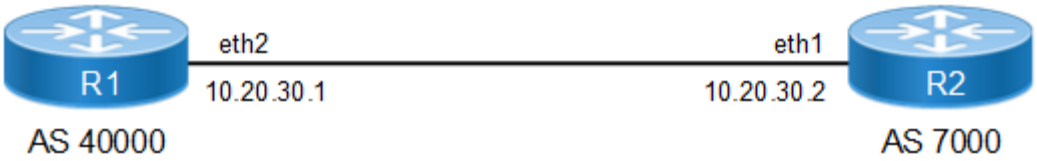


Figure 1-79: 4-Octet ASN on Both Routers

R1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 400000`	Assign the ASN value (`400000`) to the router.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).

R2

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#neighbor 10.20.30.1 remote-as 400000`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400000`).

4-Octet ASN Capability Enabled on R1 and Disabled on R2

In the following two examples, 4-Octet ASN capability is enabled on BGP speaker R1 and disabled on R2.

Topology

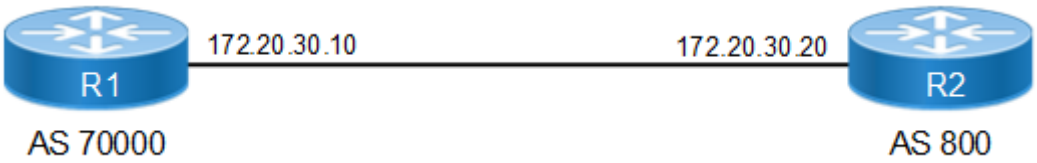


Figure 1-80: 4-Octet ASN on One Router

R1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 70000`	Assign the ASN value (`70000`) to the router.
`(config-router)#neighbor 172.20.30.20 remote-as 800`	Specify the neighbor's IP address (`172.20.30.20`) and the ASN value of the neighbor (`800`).

R2

`#configure terminal`	Enter configure mode.
`(config)#no bgp extended-asn-cap`	Disable 4-octet ASN capability.
`(config)#router bgp 800`	Assign the ASN value (`800`) to the router.
`(config-router)#neighbor 172.20.30.10 remote-as 70000`	Specify the neighbor's IP address (`172.20.30.10`) and the ASN value of the neighbor (`70000`).

Topology

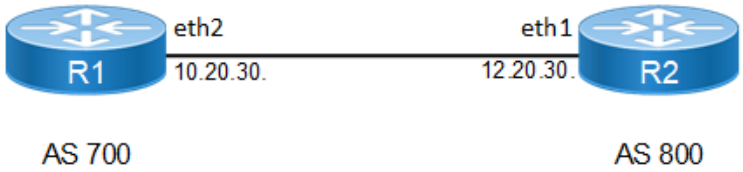


Figure 1-81: 4-Octet ASN

R1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 700`	Assign the ASN value (`700`) to the router.
`(config-router)#neighbor 172.20.30.20 remote-as 800`	Specify the neighbor's IP address (`172.20.30.20`) and the ASN value of the neighbor (`800`).

R2

`#configure terminal`	Enter configure mode.
`(config)#no bgp extended-asn-cap`	Disable 4-octet ASN capability.
`(config)#router bgp 800`	Assign the ASN value (`800`) to the router.
`(config-router)#neighbor 172.20.30.10 remote-as 700`	Specify the neighbor's IP address (`172.20.30.10`) and the ASN value of the neighbor (`700`).

Validation

```
#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4  7000    2          3       1      0      0
00:00:08              0

Total number of neighbors 1

Total number of Established sessions 1
```

```
#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400000, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:02:20
  Last read 00:00:20, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 49434
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

BGP Extended Community Attribute

The Extended Community Attribute provides a mechanism for labeling information carried in BGP.

Extended Community with a 2-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 are 2-byte-ASN capable, and do not support 4-byte-ASN capability.

Topology

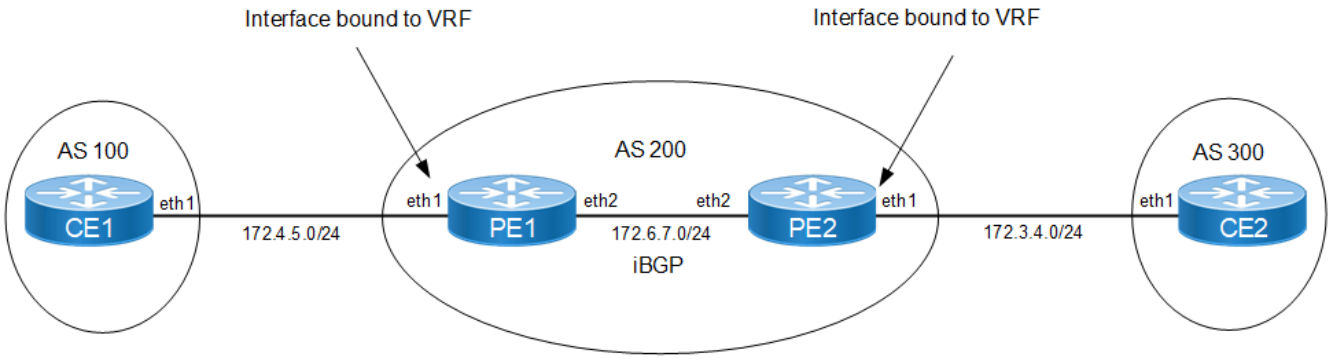


Figure 1-82: Extended Communities — 2-Byte ASN

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.4.5.116 remote-as 200`	Specify the neighbor's IP address (`172.4.5.116`) and the ASN value of the neighbor (`200`).

CE2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.3.4.114/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 300`	Assign the ASN value (`300`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.3.4.117 remote-as 200`	Specify the neighbor's IP address (`172.3.4.117`) and the ASN value of the neighbor (`200`).

PE1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 100:10`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.4.5.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 75.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 172.6.7.117 remote-as 200`	Specify the neighbor's (PE2) IP address (`172.6.7.117`) and the ASN value of the neighbor (`200`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.117 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.4.5.115 remote-as 100`	Specify the neighbor's (CE1) IP address and ASN value.
`(config-router-af)#neighbor 172.4.5.115 send-community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF.
`(config-vrf)#route-target both 100:10`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.3.4.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 100.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 172.6.7.116 remote-as 200`	Specify the neighbor's (PE1) IP address (`172.6.7.116`) and the ASN value of the neighbor (`200`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.116 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.3.4.114 remote-as 300`	Specify the neighbor's (CE2) IP address and ASN value.
`(config-router-af)#neighbor 172.3.4.114 send-community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

Validation

CE1

```
#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
```

```
!
ip domain-lookup
feature telnet
feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$AUeGhbf0$HCHhxemCQ39LPYOjC.Kb7/
feature rsyslog
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.52.2/24
!
interface eth1
 ip address 172.4.5.115/24
!
interface eth2
 shutdown
!
interface eth3
 shutdown
!
interface eth4
 shutdown
!
interface eth5
 shutdown
!
router bgp 100
 neighbor 172.4.5.116 remote-as 200
!
line con 0
 login
line vty 0 39
 login
!
end

#
#show ip bgp
BGP table version is 8, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
*>   75.1.1.0/24      172.4.5.116           0         100           0       200 ?
*>   100.1.1.0/24     172.4.5.116           0         100           0       200 ?

Total number of prefixes 2
#
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:04:22
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 131 messages, 1 notifications, 0 in queue
  Sent 129 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 8, neighbor version 8
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 37982
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:54, due to BGP Notification received
Notification Error Message: (Cease/Peer Unconfigured.)


#show ip bgp vrf all
BGP table version is 8, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   75.1.1.0/24      172.4.5.116           0         100           0       200 ?
*>   100.1.1.0/24     172.4.5.116           0         100           0       200 ?

Total number of prefixes 2
#
```

```
#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100
BGP table version is 8
1 BGP AS-PATH entries
0 BGP community entries

Neighbor               V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116            4   200  168       165      8     0     0  00:22:04
2

Total number of neighbors 1

Total number of Established sessions 1
```

PE1

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:10 (Default for VRF VRF1)
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 100:10
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1


#show ip bgp vrf all
BGP table version is 2, local router ID is 172.4.5.116
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?

Total number of prefixes 2
```

```
#show ip bgp summary vrf all
BGP router identifier 172.4.5.116, local AS number 200
BGP VRF VRF1 Route Distinguisher: 100:10
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.115             4   100   55        60      2     0     0  00:26:54
0

Total number of neighbors 1

Total number of Established sessions 1
BGP router identifier 192.168.52.3, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.6.7.117             4   200   80       101      1     0     0  00:37:47
0

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 172.6.7.117, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.5
  BGP state = Established, up for 00:38:33
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 82 messages, 0 notifications, 0 in queue
  Sent 103 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

```
 For address family: VPNv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.6.7.116, Local port: 179
Foreign host: 172.6.7.117, Foreign port: 57743
Nexthop: 172.6.7.116
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 172.4.5.115, vrf VRF1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 172.4.5.116, remote router ID 192.168.52.2
  BGP state = Established, up for 00:27:40
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 57 messages, 0 notifications, 0 in queue
  Sent 62 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.116, Local port: 37982
Foreign host: 172.4.5.115, Foreign port: 179
Nexthop: 172.4.5.116
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp vrf all
BGP table version is 2, local router ID is 172.4.5.116
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
```



```
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?

Total number of prefixes 2
```

PE2

```
#show ip bgp vrf all
BGP table version is 1, local router ID is 172.3.4.117
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>i  75.1.1.0/24      172.6.7.116          0         100           0        ?
*>   100.1.1.0/24     0.0.0.0             0         100           32768    ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 172.3.4.117, local AS number 200
BGP VRF VRF1 Route Distinguisher: 100:10
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor               V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.3.4.114            4   300   82        85      1     0     0  00:40:05
0

Total number of neighbors 1

Total number of Established sessions 1
BGP router identifier 192.168.52.5, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor               V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.6.7.116            4   200  113       113      1     0     0  00:54:07
0

Total number of neighbors 1

Total number of Established sessions 1#
```

```
#show ip bgp neighbors
BGP neighbor is 172.6.7.116, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  BGP state = Established, up for 00:56:09
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 117 messages, 0 notifications, 0 in queue
  Sent 117 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.6.7.117, Local port: 57743
Foreign host: 172.6.7.116, Foreign port: 179
Nexthop: 172.6.7.117
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 172.3.4.114, vrf VRF1, remote AS 300, local AS 200, external link
  BGP version 4, local router ID 172.3.4.117, remote router ID 192.168.52.4
  BGP state = Established, up for 00:42:07
  Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 86 messages, 0 notifications, 0 in queue
  Sent 89 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
```

```
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.117, Local port: 54753
Foreign host: 172.3.4.114, Foreign port: 179
Nexthop: 172.3.4.117
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

CE2

```
    #show ip bgp vpnv4 all
    #show ip bgp
    BGP table version is 3, local router ID is 192.168.52.4
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal,
                  l - labeled, S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path
    *>   75.1.1.0/24      172.3.4.117           0         100           0       200
    ?
    *>   100.1.1.0/24     172.3.4.117           0         100           0       200
    ?

    Total number of prefixes 2
    #
    #
    #show ip bgp vrf all
    BGP table version is 3, local router ID is 192.168.52.4
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal,
                  l - labeled, S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path
    *>   75.1.1.0/24      172.3.4.117           0         100           0       200
    ?
    *>   100.1.1.0/24     172.3.4.117           0         100           0       200
    ?

    Total number of prefixes 2
    #
    #
    #show ip bgp summary vrf all
    BGP router identifier 192.168.52.4, local AS number 300
    BGP table version is 3
    1 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
    Down    State/PfxRcd
```

```
172.3.4.117              4   200  382        414       3      0      0
00:42:54              2

Total number of neighbors 1

Total number of Established sessions 1
#
#
#show ip bgp neighbors
BGP neighbor is 172.3.4.117, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 192.168.52.4, remote router ID 172.3.4.117
  BGP state = Established, up for 00:43:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 236 messages, 147 notifications, 0 in queue
  Sent 415 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.114, Local port: 179
Foreign host: 172.3.4.117, Foreign port: 54753
Nexthop: 172.3.4.114
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:43:32, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#
```

Extended Community with a 4-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 support 4-byte ASN capability.

Note: PE1 and PE2 should both either be 4-byte-ASN capable or 2-byte-ASN capable. Support for the combination of one 4-byte-ASN capable PE with one 2-byte-ASN-capable PE is currently unavailable.

Topology

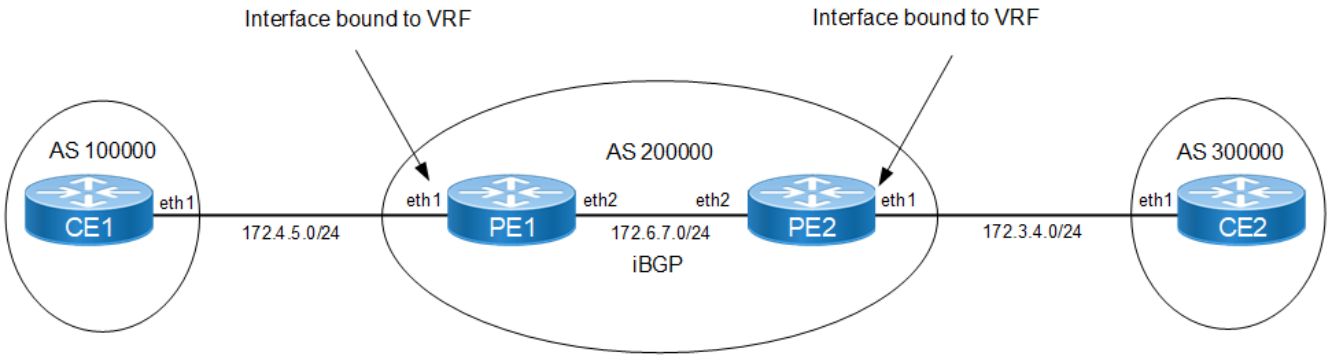


Figure 1-83: Extended Communities — 4-Byte ASN

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 100000`	Assign the ASN value (`100000`) to the router. The ASN range is <1-4294967295>.
`(config-router)#neighbor 172.4.5.116 remote-as 200000`	Specify the neighbor's IP address (`172.4.5.116`) and the ASN value of the neighbor (`200000`).

PE1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability. Dynamic change from 2-byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 1.1.1.1:200`	Assign a 4-byte route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in A.B.C.D:NN format.
`(config-vrf)#route-target both 1.1.1.1:200`	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.4.5.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 50.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200000`	Assign the ASN value (`200000`) to the router.
`(config-router)#neighbor 172.6.7.117 remote-as 200000`	Specify the neighbor's (PE2) IP address (`172.6.7.117`) and the ASN value of the neighbor (`200000`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.117 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.4.5.115 remote-as 100000`	Specify the neighbor's (CE1) IP address and ASN value.
`(config-router-af)#neighbor 172.4.5.115 send-community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

PE2

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability. Dynamic change from 2-byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 1.1.1.1:200`	Assign a 4-byte route distinguisher (RD) for the VRF.
`(config-vrf)#route-target both 1.1.1.1:200`	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.3.4.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 200.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200000`	Assign the ASN value (`200000`) to the router.
`(config-router)#neighbor 172.6.7.116 remote-as 200000`	Specify the neighbor's (PE2) IP address (`172.6.7.116`) and the ASN value of the neighbor (`200000`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.116 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.3.4.114 remote-as 300000`	Specify the neighbor's (CE1) IP address and ASN value.
`(config-router-af)#neighbor 172.3.4.114 send-community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

CE2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.3.4.114/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 300000`	Assign the ASN value (`300000`) to the router.
`(config-router)#neighbor 172.3.4.117 remote-as 200000`	Specify the neighbor's IP address (`172.3.4.117`) and the ASN value of the neighbor (`200000`).

Validation

CE1

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp vrf all
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.4.5.116           0         100           0       200000 ?
*>   200.1.1.0        172.4.5.116           0         100           0       200000 ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116             4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1

Total number of Established sessions 1
```

PE1

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

```
#show ip bgp vrf all
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.4.5.116           0         100           0       200000 ?
*>   200.1.1.0        172.4.5.116           0         100           0       200000 ?

Total number of prefixes 2

#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116            4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1

Total number of Established sessions 1


#clear bgp *
2019 Mar 22 06:16:56.414 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]: Neighbour
[172.4.5.116] Session down due to peer clear
```

PE2

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
```

```
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp vrf all
BGP table version is 1, local router ID is 172.3.4.117
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>i  50.1.1.0/24      172.6.7.116          0         100           0        ?
*>   200.1.1.0        0.0.0.0             0         100          32768    ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116            4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1

Total number of Established sessions 1


#clear bgp *
2019 Mar 22 06:16:56.414 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]: Neighbour
[172.4.5.116] Session down due to peer clear
```

CE2

```
#show ip bgp vrf all
BGP table version is 4, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.3.4.117           0         100           0       200000 ?
*>   200.1.1.0        172.3.4.117           0         100           0       200000 ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.4, local AS number 300000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.3.4.117             4 200000   33        30      4     0     0  00:04:34
2

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 172.3.4.117, remote AS 200000, local AS 300000, external link
  BGP version 4, local router ID 192.168.52.4, remote router ID 172.3.4.117
  BGP state = Established, up for 00:04:40
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 33 messages, 0 notifications, 0 in queue
  Sent 29 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
```

```
Local host: 172.3.4.114, Local port: 179
Foreign host: 172.3.4.117, Foreign port: 49361
Nexthop: 172.3.4.114
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:40, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)
```

Nexthop Tracking

Nexthop tracking is used to notify the BGP process asynchronously whenever there is any change in the IGP routes. It reduces the convergence time of BGP routes when IGP routes are changed.

Topology

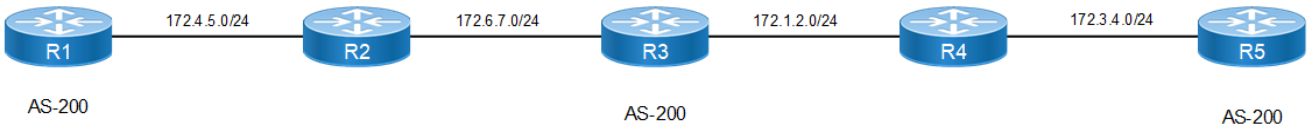


Figure 1-84: BGP Nexthop Tracking

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 100.100.100.100/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (200.200.200.200) and the ASN value of the neighbor (200).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area 0.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if) #ip address 150.150.150.150/32 secondary`	Configure the IP address on this interface.
`(config-if)#ip address 200.200.200.200/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 100.100.100.100 remote-as 200`	Specify the neighbor's IP address (`100.100.100.100`) and the ASN value of the neighbor (`200`).
`(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200`	Specify the routing update source.
`(config-router)#neighbor 220.220.220.220 remote-as 200`	Specify the neighbor's IP address (`220.220.220.220`) and the ASN value of the neighbor (`200`).
`(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#network 172.1.2.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#redistribute connected`	Redistribute the connected routes.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#bgp nexthop-trigger enable`	Enable Nexthop tracking.
`(config)#bgp nexthop-trigger delay 20`	Configure the nexthop trigger-delay time interval.

R4

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`(config-router)#network 172.1.2.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#network 172.3.4.0/24 area 0`	Advertise the network in Area `0`.

R5

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 220.220.220.220/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 150.150.150.150 remote-as 200`	Specify the neighbor's IP address (150.150.150.150) and the ASN value of the neighbor (`200`).

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 220.220.220.220/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config-router)#neighbor 150.150.150.150 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.3.4.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

Validation

show ip bgp summary, show ip bgp neighbors, show bgp nexthop-tracking, show ip bgp scan

Nexthop Tracking Delay Timer

The delay interval between routing table walks can be configured for nexthop delay tracking. This time determines how long BGP waits before it starts walking the full BGP routing table after receiving notification from NSM about a next-hop change.

Topology

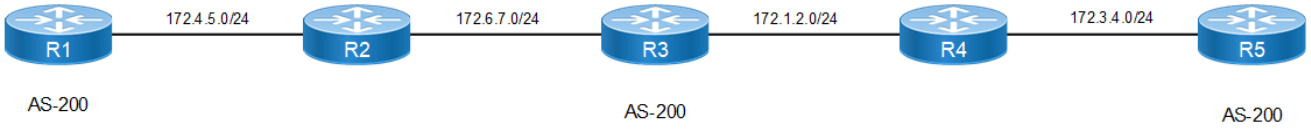


Figure 1-85: Topology for Nexthop Tracking Delay Timer

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 150.150.150.150/32 secondary`	Configure the IP address on this interface.
`(config-if)#ip address 100.100.100.100/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (200.200.200.200) and the ASN value of the neighbor (200).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 150.150.150.150/32 secondary`	Configure the IP address on this interface.
`(config-if)#ip address 100.100.100.100/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area 0.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 200.200.200.200/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router.
`(config-router)#neighbor 100.100.100.100 remote-as 200`	Specify the neighbor's IP address (100.100.100.100) and the ASN value of the neighbor (200).
`(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200`	Specify the routing update source.
`(config-router)#neighbor 220.220.220.220 remote-as 200`	Specify the neighbor's IP address (220.220.220.220) and the ASN value of the neighbor (200).
`(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#network 172.1.2.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#bgp nexthop-trigger enable`	Enable nexthop tracking.
`(config)#bgp nexthop-trigger delay 20`	Configure the nexthop trigger-delay time interval.

R4

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.1.2.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#network 172.3.4.0/24 area 0`	Advertise the network in Area 0.

R5

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 220.220.220.220/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router.
`(config-router)#neighbor 150.150.150.150 remote-as 200`	Specify the neighbor's IP address (150.150.150.150) and the ASN value of the neighbor (200).
`(config-router)#neighbor 150.150.150.150 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.3.4.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

Validation

R1

```
#show ip bgp summary
BGP router identifier 10.12.20.71, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
200.200.200.200          4   200   15         16       1      0      0
00:06:37              0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 200.200.200.200, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 10.12.20.71, remote router ID 200.200.200.200
  BGP state = Established, up for 00:06:40
  Last read 00:06:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 15 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 100.100.100.100, Local port: 37676
Foreign host: 200.200.200.200, Foreign port: 179
Nexthop: 100.100.100.100
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 10.12.20.71

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60
scan remain-time: 38
Current BGP nexthop cache:
```

R3

```
#show ip bgp summary
BGP router identifier 200.200.200.200, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
100.100.100.100           4   200   17         19       1      0      0
00:07:41               0
220.220.220.220           4   200   95        101       1      0      0
00:07:12               0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 100.100.100.100, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 200.200.200.200, remote router ID 10.12.20.71
  BGP state = Established, up for 00:07:46
  Last read 00:07:46, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
```

```
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 19 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is 200.200.200.200
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 200.200.200.200, Local port: 179
Foreign host: 100.100.100.100, Foreign port: 37676
Nexthop: 200.200.200.200
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 220.220.220.220, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 220.220.220.220
  local router ID 200.200.200.200
  BGP state = Established, up for 00:07:17
  Last read 00:07:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 94 messages, 1 notifications, 0 in queue
  Sent 97 messages, 4 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is 150.150.150.150
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 150.150.150.150, Local port: 39831
Foreign host: 220.220.220.220, Foreign port: 179
Nexthop: 150.150.150.150
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:07:22, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show bgp nexthop-tracking
Configured NHT: ENABLED
NHT Delay time-interval : 20
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 200.200.200.200
NHT is Enabled
```

```
    Recvd Msg count from RIB: 0
    NHT delay-timer remaining seconds: 0
    BGP nexthop(s):
    Total number of IPV4 nexthops : 0
    Total number of IPV6 nexthops : 0

    #show ip bgp scan
    BGP VRF: (Default) VRF_ID 0
    BGP scan interval is 60
    scan remain-time: 11
    Current BGP nexthop cache:
```

R5

```
    #show ip bgp summary
    BGP router identifier 220.220.220.220, local AS number 200
    BGP table version is 1
    0 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
    Down   State/PfxRcd
    150.150.150.150          4   200   99        101       1      0      0
    00:08:26               0

    Total number of neighbors 1

    Total number of Established sessions 1

    #show ip bgp neighbors
    BGP neighbor is 150.150.150.150, remote AS 200, local AS 200, internal link
      BGP version 4, local router ID 220.220.220.220, remote router ID
    200.200.200.200
      BGP state = Established, up for 00:08:29
      Last read 00:08:29, hold time is 90, keepalive interval is 30 seconds
      Neighbor capabilities:
        Route refresh: advertised and received (old and new)
        Address family IPv4 Unicast: advertised and received
      Received 96 messages, 3 notifications, 0 in queue
      Sent 99 messages, 2 notifications, 0 in queue
      Route refresh request: received 0, sent 0
      Minimum time between advertisement runs is 5 seconds
      Update source is lo
     For address family: IPv4 Unicast
      BGP table version 1, neighbor version 1
      Index 1, Offset 0, Mask 0x2
      Community attribute sent to this neighbor (both)
      0 accepted prefixes
      0 announced prefixes

     Connections established 6; dropped 5
    Local host: 220.220.220.220, Local port: 179
    Foreign host: 150.150.150.150, Foreign port: 39831
    Nexthop: 220.220.220.220
    Nexthop global: ::
    Nexthop local: ::
    BGP connection: non shared network
    Last Reset: 00:08:34, due to BGP Notification sent
```

```
Notification Error Message: (Cease/Other Configuration Change.)

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 220.220.220.220

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60
scan remain-time: 22
Current BGP nexthop cache:
```

BGP Distance

Administrative distance in BGP can be configured for a specific address family.

Topology

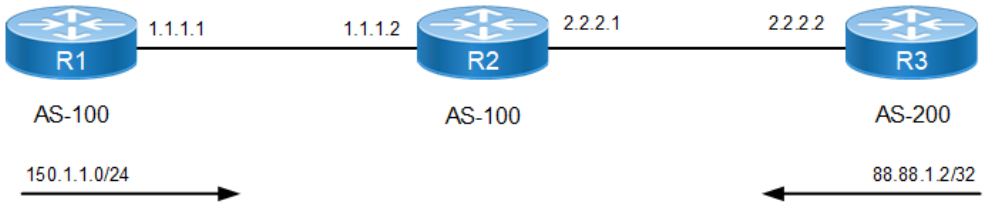


Figure 1-86: Administrative Distance for IPv4 BGP

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 150.1.1.1/24 secondary`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#network 150.1.1.0/24`	Specify the network to be advertised by the BGP routing process.
`(config-router)#neighbor 1.1.1.2 remote-as 100`	Specify the neighbor's IP address and ASN value.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 2.2.2.2 remote-as 200`	Specify the neighbor's IP address and ASN value.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Specify the neighbor's IP address and the ASN value of another neighbor.

(config-router)#distance bgp 12 13 120	Configure the administrative distance for external, internal, and local routes received.
(config-router)#aggregate-address 150.1.0.0/16 summary-only	Configure a non-AS-set aggregate route on R2. The local distance is applied to this route.

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 88.88.1.2/32 secondary	Specify IP address for the interface.
(config-if)#exit	Exit loopback interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#network 88.88.1.2/32	Specify the network to be advertised by the BGP routing process.
(config-router)#neighbor 2.2.2.1 remote-as 100	Specify the neighbor's IP address and ASN value.

Validation

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 100
BGP table version is 7
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
1.1.1.1                  4   100    8          9       7      0      0
00:02:39               1
2.2.2.2                  4   200    4          4       7      0      0
00:00:38               1

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 150.1.1.1
  BGP state = Established, up for 00:02:54
  Last read 00:02:54, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 7, neighbor version 7
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
```

```
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 49238
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:fea6:6e3
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 2.2.2.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 88.88.1.2
  local router ID 192.168.52.3
  BGP state = Established, up for 00:00:53
  Last read 00:00:53, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 7, neighbor version 7
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 50072
Nexthop: 2.2.2.1
Nexthop global: fe80::a00:27ff:fe77:264e
Nexthop local: ::
BGP connection: non shared network

#show ip route database bgp
IP Route Table for VRF "default"
B    *> 88.88.1.2/32 [12/0] via 2.2.2.2, eth2, 00:01:19
B    *> 150.1.0.0/16 [120/0] is a summary, Null, 00:02:49
B    *> 150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:02:49

Gateway of last resort is not set
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  1.1.1.0/24 is directly connected, eth1, 00:13:39
C    *>  2.2.2.0/24 is directly connected, eth3, 00:13:04
```

```
B    *>  88.88.1.2/32 [12/0] via 2.2.2.2, eth3, 00:06:37
C    *>  127.0.0.0/8 is directly connected, lo, 00:22:15
B    *>  150.1.0.0/16 [120/0] is a summary, Null, 00:11:19
B    *>  150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:11:19
C    *>  192.168.52.0/24 is directly connected, eth0, 00:22:13

Gateway of last resort is not set

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:17:38
C     2.2.2.0/24 is directly connected, eth3, 00:17:03
B     88.88.1.2/32 [12/0] via 2.2.2.2, eth3, 00:10:36
C     127.0.0.0/8 is directly connected, lo, 00:26:14
B     150.1.0.0/16 [120/0] is a summary, Null, 00:15:18
B     150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:15:18
C     192.168.52.0/24 is directly connected, eth0, 00:26:12

Gateway of last resort is not set

#show ip bgp
BGP table version is 4, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   88.88.1.2/32     2.2.2.2              0         100           0       200
i
*>   150.1.0.0        0.0.0.0             0         100           32768    i
s>i  150.1.1.0/24     1.1.1.1              0         100           0        i

Total number of prefixes 3
```

BGP Weight per Peer

A different weight can be assigned per address family of a peer. For example, a system can be configured to prefer VPN4 routes from peer A and IPv4 routes from peer B.

If the neighbor weight command is given under a specific address-family mode, the peer weight is set for that specific address family. If the address family is not specifically set, the weight is updated for the default address-family.

Topology

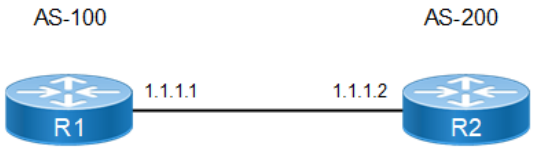


Figure 1-87: BGP Weight Per Peer

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Specify the neighbor's IP address and ASN value.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#neighbor 1.1.1.1 weight 500`	Add a weight of `500` to all the routes coming from the neighbor, `1.1.1.1` (only IPv4 routes).

Validation

R1

```
#show ip bgp summary
BGP router identifier 192.168.56.101, local AS number 100
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
n State/PfxRcd
1.1.1.2 4 200 6 7 1 0 0 00:02:00
0
Total number of neighbors 1
Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 34619
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:09:10
C     127.0.0.0/8 is directly connected, lo, 00:15:56
C     192.168.52.0/24 is directly connected, eth0, 00:15:52

Gateway of last resort is not set
```

R2

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
n State/PfxRcd
1.1.1.1 4 100 3 3 1 0 0 00:00:34
0
Total number of neighbors 1
Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:07:14
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
```

```
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
 Weight500
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 34619
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:11:26
C     127.0.0.0/8 is directly connected, lo, 00:21:36
C     192.168.52.0/24 is directly connected, eth0, 00:21:32

Gateway of last resort is not set
```

OSPF as PE-CE Protocol for VPNs

In an MPLS VPN environment, customer networks are connected to an MPLS VPN-enabled provider backbone. As shown in Figure 1-88, Customer A areas, Areas 0 and 1, are connected to an MPLS VPN–enabled provider network. Area 0 and Area 1 have routers CE1 and CE2 running OSPF. MP-iBGP is used between PE1 and PE2 to propagate routes between Site 1 (Area 0) and Site 2 (Area 1). Traditional OSPF-BGP redistribution is performed at PE routers, PE1 and PE2. In this case, routes distributed by CE1 into the MP-iBGP cloud are sent to CE2 as external routes, even though both CE1 and CE2 belong to the same customer.

This behavior can be changed with the additional domain ID configuration. Each VRF should be configured a domain ID on the PE routers. If a PE router gets a route through the MP-iBGP cloud and has to send to any customer site, it checks the domain ID value against the list of stored domain ID values. If the incoming domain ID matches any of the stored IDs, that route is inserted into the customer site with the same type, as it was inserted into the MP-BGP cloud; otherwise, it is inserted as external route.

Topology

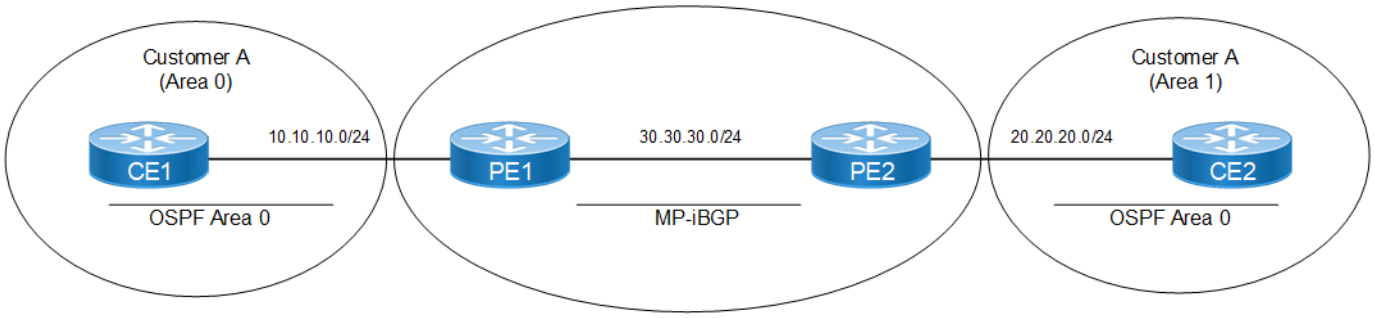


Figure 1-88: OSPF as PE-CE Protocol

CE1

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 60.1.1.1/24 secondary`	Specify IP address for the interface
`(config-if)#exit`	Exit loopback interface mode
`(config)#router ospf 1`	Configure the routing process and specify the Process ID (1).
`(config-router)#network 10.10.10.0/24 area 0`	Advertise the network in OSPF
`(config-router)#network 60.1.1.0/24 area 0`	Advertise the loopback IP address in area 0 of router OSPF 1.

PE1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf ABC`	Specify the name of the VRF (ABC) to be created.
`(config-vrf)#rd 10:100`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 10:100`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding ABC`	Associate interface eth1 to vrf ABC.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1 ABC`	Configure OSPF for VRF.
`(config-router)#network 10.10.10.0/24 area 0`	Advertise the network for OSPF adjacency with CE1.
`(config-router)#domain-id 1.1.1.1`	Configure the primary domain ID.
`(config-router)#domain-id 2.2.2.2 secondary`	Configure a secondary domain ID.
`(config-router)#domain-id 3.3.3.3 secondary`	Configure a secondary domain ID.
`(config-router)#exit`	Exit Router mode and return to Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the BGP router.

(config-router)#neighbor 30.30.30.2 remote-as 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.2 activate	Activate neighbor 30.30.30.2.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

PE2

#configure terminal	Enter configure mode.
(config)#ip vrf ABC	Specify the name of the VRF (ABC) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 10:100	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding ABC	Associate interface eth1 to vrf ABC.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1 ABC	Configure OSPF for VRF.
(config-router)#network 20.20.20.0/24 area 0	Advertise the network for OSPF adjacency with CE1.
(config-router)#domain-id 1.1.1.1	Configure the primary domain ID.
(config-router)#domain-id 2.2.2.2 secondary	Configure a secondary domain ID.
(config-router)#domain-id 3.3.3.3 secondary	Configure a secondary domain ID.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 30.30.30.1 remote-as 100	Configure neighbor 30.30.30.1 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.1 activate	Activate neighbor 30.30.30.1.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

CE2

#configure terminal	Enter configure mode.

`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1).
`(config-router)#network 20.20.20.0/24 area 0`	Advertise the network in OSPF.

Validation

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 10:100 (Default for VRF ABC)
*>   10.10.10.0/24    0.0.0.0               2         100           32768    ?
*>   60.1.1.1/32      10.10.10.1            12        100           32768    ?
 Announced routes count = 2
 Accepted routes count = 0
#
```

BGP Multipath for IPv4

BGP supports multipath for IPv4 prefixes. BGP Multipath allows load-balancing traffic among multiple BGP routes. It supports both iBGP and eBGP routes. In case of eBGP, the routes should arrive from same AS number.

Topology

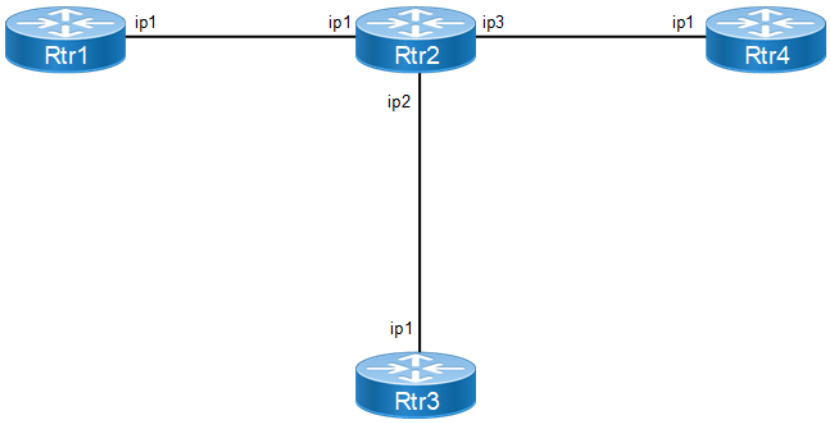


Figure 1-89: Multipath iBGP for IPv4

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#redistribute static`	Redistribute the static routes.

(config-router)#neighbor 30.30.30.9 remote-as 100	Configure neighbor 30.30.30.9 for iBGP.
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr3

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#bgp router-id 4.4.4.4	Configure a fixed Router ID (4.4.4.4).
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 40.40.40.9 remote-as 100	Configure neighbor 40.40.40.9 for iBGP.
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr4

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#bgp router-id 6.6.6.6	Configure a fixed Router ID (6.6.6.6).
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 50.50.50.9 remote-as 100	Configure neighbor 50.50.50.9 for iBGP.
(config)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#max-paths ibgp 2	Configure iBGP max-paths (2).
(config)#bgp router-id 9.9.9.9	Configure a fixed Router ID (9.9.9.9).
(config-router)#neighbor 30.30.30.2 remote-as 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#neighbor 40.40.40.4 remote-as 100	Configure neighbor 40.40.40.4 for iBGP.
(config-router)#neighbor 50.50.50.6 remote-as 100	Configure neighbor 50.50.50.6 for iBGP.
(config-router)#exit	Exit the Router mode and return to Configure mode.

Validation

```
#show ip bgp 88.88.0.0
BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #1, table Default-IP-Routing-Table)
```

```
  Not advertised to any peer
  Local
    30.30.30.2 from 30.30.30.2 (2.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, multipath-
candidate, installed, best
      Last update: Wed Mar  2 15:17:38 2016

  Local
    50.50.50.6 from 50.50.50.6 (6.6.6.6)
      Origin incomplete, metric 0, localpref 100, valid, internal, multipath-
candidate
      Last update: Wed Mar  2 15:23:58 2016

  Local
    40.40.40.4 from 40.40.40.4 (4.4.4.4)
      Origin incomplete, metric 0, localpref 100, valid, internal, multipath-
candidate, installed
      Last update: Wed Mar  2 15:21:45 2016

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     30.30.30.0/24 is directly connected, eth1, 00:15:04
C     40.40.40.0/24 is directly connected, eth6, 00:14:30
C     50.50.50.0/24 is directly connected, eth3, 00:14:46
B     88.88.0.0/16 [200/0] via 40.40.40.4, eth6, 00:02:58
            [200/0] via 30.30.30.2, eth1
C     127.0.0.0/8 is directly connected, lo, 00:19:21
C     192.168.52.0/24 is directly connected, eth0, 00:19:16

Gateway of last resort is not set

Gateway of last resort is not set

#show running-config router bgp
!
router bgp 100
 bgp router-id 9.9.9.9
 max-paths ibgp 2
 neighbor 30.30.30.2 remote-as 100
 neighbor 40.40.40.4 remote-as 100
 neighbor 50.50.50.6 remote-as 100
!
#
```

Multipath eBGP

Topology

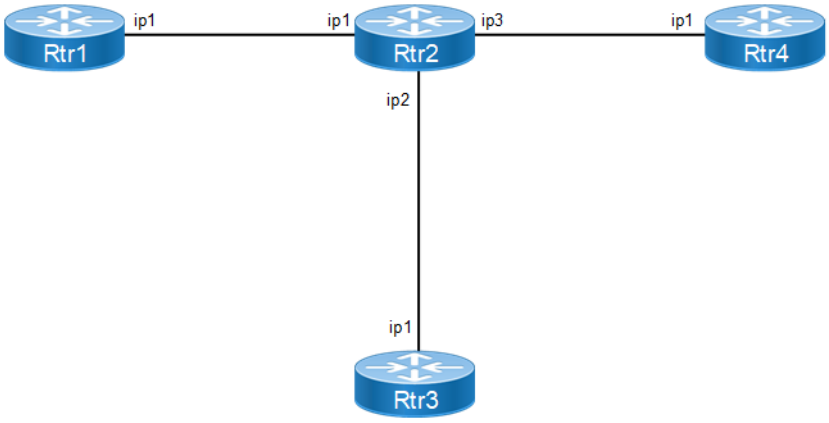


Figure 1-90: Multipath eBGP for IPv4

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 30.30.30.9 remote-as 100`	Configure neighbor 30.30.30.9 for eBGP.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr3

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 4.4.4.4`	Configure a fixed Router ID (4.4.4.4).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 40.40.40.9 remote-as 100`	Configure neighbor 40.40.40.9 for eBGP.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr4

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.

(config-router)#bgp router-id 6.6.6.6	Configure a fixed Router ID (6.6.6.6).
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 50.50.50.9 remote-as 100	Configure neighbor 50.50.50.9 for eBGP.
(config)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#max-paths ebgp 2	Configure eBGP max-paths (2).
(config)#bgp router-id 9.9.9.9	Configure a fixed Router ID (9.9.9.9).
(config-router)#neighbor 30.30.30.2 remote-as 200	Configure neighbor 30.30.30.2 for eBGP.
(config-router)#neighbor 40.40.40.4 remote-as 200	Configure neighbor 40.40.40.4 for eBGP.
(config-router)#neighbor 50.50.50.6 remote-as 200	Configure neighbor 50.50.50.6 for eBGP.
(config-router)#exit	Exit the Router mode and return to Configure mode.

Validation

```
#show ip bgp 88.88.0.0

BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #3, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  30.30.30.2 50.50.50.6
  200
    30.30.30.2 from 30.30.30.2 (2.2.2.2)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate,
installed
      Last update: Sat Jan  3 02:06:25 1970

  200
    50.50.50.6 from 50.50.50.6 (6.6.6.6)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate
      Last update: Sat Jan  3 02:05:39 1970

  200
    40.40.40.4 from 40.40.40.4 (4.4.4.4)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate,
installed, best
      Last update: Sat Jan  3 02:05:11 1970

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     30.30.30.0/24 is directly connected, eth1, 05:26:26
C     40.40.40.0/24 is directly connected, eth6, 05:25:52
C     50.50.50.0/24 is directly connected, eth3, 05:26:08
B     88.88.0.0/16 [20/0] via 40.40.40.4, eth6, 00:01:38
            [20/0] via 30.30.30.2, eth1
C     127.0.0.0/8 is directly connected, lo, 05:30:43
C     192.168.52.0/24 is directly connected, eth0, 05:30:38

Gateway of last resort is not set

#show running-config router bgp
!
router bgp 100
 bgp router-id 9.9.9.9
 max-paths ebgp 2
 neighbor 30.30.30.2 remote-as 200
 neighbor 40.40.40.4 remote-as 200
 neighbor 50.50.50.6 remote-as 200
!
```

BGP AS-PATH Multipath-relax

BGP will not load balance across multiple paths by default. We can configure it to do so with the `max-paths ebgp <no-of-multipaths>` command. The criterion of this command is that all attributes must match (Weight, Local preference, AS Path, etc). This is acceptable if we are multi-homed to a single AS, but what if we are multi-homed to different AS.

BGP AS PATH multipath relax effectively allows for ECMP to be done across different neighboring ASN's.

Topology

Below topology explains about BGP AS PATH multipath relax functionality.

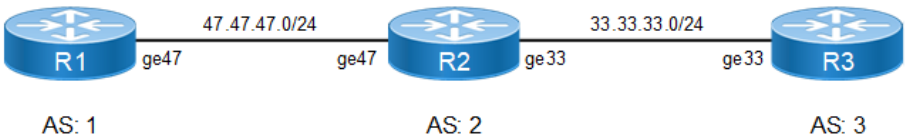


Figure 1-91: BGP AS-PATH Multipath-relax Topology

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter Interface loopback
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for interface
`(config-if)#exit`	Exit interface mode
`(config)#interface ge47`	Enter Interface loopback
`(config-if)#ip address 47.47.47.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter the Configure mode
`(config)#router bgp 1`	Assign the ASN value (1) to the BGP router
`(config-router)#neighbor 47.47.47.2 remote-as 2`	Configure eBGP neighbor.
`(config-router)#network 100.1.1.0/24`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from BGP router config mode

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface ge33`	Enter interface mode
`(config-if)#ip address 33.33.33.2/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter the Configure mode
`(config)#interface ge47`	Enter interface mode
`(config-if)#ip address 47.47.47.2/24`	Configure IP address for interface.
`(config-if)#exit`	Exit from interface mode and enter the Configure mode
`(config)#router bgp 2`	Assign the ASN value (2) to the BGP router.
`(config-router)#neighbor 33.33.33.3 remote-as 3`	Configure eBGP neighbor.
`(config-router)#neighbor 47.47.47.1 remote-as 1`	Configure eBGP neighbor.
`(config-router)#max-paths ebgp 8`	Configure eBGP Multipath.
`(config-router)#bgp bestpath as-path multipath-relax`	Configure BGP AS PATH Multipath relax.
`(config-router)#end`	Exit from BGP router config mode.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter Interface loopback.
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for interface.
`(config-if)#exit`	Exit from interface mode and enter the Configure mode.
`(config)#interface ge33`	Enter Interface loopback.
`(config-if)#ip address 33.33.33.3/24`	Configure IP address for interface.

(config-if)#exit	Exit from interface mode and enter the Configure mode.
(config)#router bgp 3	Assign the ASN value (3) to the BGP router.
(config-router)#neighbor 33.33.33.2 remote-as 2	Configure eBGP neighbor.
(config-router)#network 100.1.1.0/24	Advertise the loopback network into BGP.
(config-router)#end	Exit from BGP router config mode.

Validation

```
R2#show running-config bgp
!
router bgp 2
 bgp bestpath as-path multipath-relax
 max-paths ebgp 8
 neighbor 33.33.33.3 remote-as 3
 neighbor 47.47.47.1 remote-as 1
!
R2#show ip bgp 100.1.1.0
BGP routing table entry for 100.1.1.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  47.47.47.1
  3
    33.33.33.3 from 33.33.33.3 (33.33.33.3)
      Origin IGP, metric 0, localpref 100, valid, external, multipath-
candidate, installed, best
      Last update: Tue Feb 23 03:13:14 2016
  1
    47.47.47.1 from 47.47.47.1 (62.57.1.1)
      Origin IGP, metric 0, localpref 100, valid, external, multipath-
candidate, installed
      Last update: Tue Feb 23 03:13:15 2016

R2#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 2
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries
8  Configured ebgp ECMP multipath: Currently set at 8
1  Configured ibgp ECMP multipath: Currently set at 1
1  Configured eibgp ECMP multipath: Currently set at 1

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
33.33.33.3               4     3    5          6       2      0      0
00:01:10              1
47.47.47.1               4     1   16         15       2      0      0
00:06:33              1

Total number of neighbors 2

Total number of Established sessions 2


R2#show ip bgp
```

```
BGP table version is 2, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.1.1.0/24     47.47.47.1            0         100           0       1 i
*                     33.33.33.3            0         100           0       3 i

Total number of prefixes 1
```

BGP FIB Install (Selective Route Download)

The BGP—Selective Route Download feature allows a network administrator to selectively download some or none of the BGP routes into the Routing Information Base (RIB). The primary application for this feature is to suppress the unnecessary downloading of certain BGP routes to the RIB or Forwarding Information Base (FIB) on a dedicated route reflector, which propagates BGP updates without carrying transit traffic. The feature thereby helps to maximize resources available and to improve routing scalability and convergence on the dedicated route reflector.

With RFC 4456, the concept of route reflection was defined; this would allow configuring designated one or more BGP routers in iBGP network as route reflectors. BGP relaxes the re-advertising restriction on these route reflectors, allowing them to accept and propagate IBGP routes to their clients.

The role of a dedicated route reflector (RR) is to propagate BGP updates without participating in the actual forwarding of transit traffic. That means the RR does not need to have all BGP routes downloaded into its RIB or FIB. It is beneficial for the RR to preserve its resources by not processing and storing those routes.

By default, BGP routes are downloaded to the RIB. To save resources on a dedicated route reflector, such downloading can be reduced or prevented by configuring a table map. A table map is so named because it controls what is put into the BGP routing table.

By reducing the route installation in the dedicated route reflectors, we can maximize availability of resources and improve routing scalability and convergence.

A new command ‘table map’ is being introduced to achieve this. A table map controls what is put into the BGP routing table. When configured it would reduce or prevent downloading routes to RIB.

Table map command references ‘route map’ rules available in BGP to control the routes going into the BGP routing table.

Table-map command can be used in two ways:

- When a simple table-map command is given (without filter option), the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option ‘filter’ is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Topology

Below topology explains about BGP FIB Install functionality

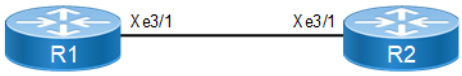


Figure 1-92: BFP FIB Install Topology

R1

#configure terminal	Enter the Configure mode.
(config)#interface xe3/1	Enter interface mode.
(config-if)#ip address 20.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit interface mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 20.1.1.2 remote-as 100	Configure neighbor in IBGP
(config-router)#redistribute static	Redistribute static routes to advertise to its neighbor
(config-router)#exit	Exit Router mode and enter Configure mode
(config)#ip route 1.1.1.0/24 xe3/1	Configure static route.
(config)#ip route 2.2.2.0/24 xe3/1	Configure static route.
(config)#ip route 3.3.3.0/24 xe3/1	Configure static route.
(config)#ip route 4.4.4.0/24 xe3/1	Configure static route.
(config)#ip route 5.5.5.0/24 xe3/1	Configure static route.
(config)#ip route 6.6.6.0/24 xe3/1	Configure static route.

R2

#configure terminal	Enter the Configure mode.
(config)#interface xe3/1	Configure IP address for interface
(config-if)#ip address 20.1.1.2/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 20.1.1.1 remote-as 100	Configure neighbor iBGP.
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip access-list 1	Login to Configure access-list parameters
(config-ip-acl)#permit ipip 2.2.2.0 0.0.0.225 any	Configure access-list by allowing only one route to install in FIB table.
(config-ip-acl)#exit	Exit assess list mode
(config)# route-map test permit 1	Configure route-map to match access-list
(config-route-map)# match ip address 1	Match the above configured access-list 1
(config-route-map)#exit	Exit from route-map Configure mode and enter into Configure mode
(config)#router bgp 100	Enter into BGP router mode

(config-router)# table-map test filter	Apply table-map with route-map created and with filter option
(config-router)#end	Exit from router and Configure mode

Validation

Table-map with Filter Option

Verify BGP neighborship is up between R1 and R2. Before applying table-map in R2, all routes will be installed in FIB table, as in below output.

R1

```
#show ip bgp summary
BGP router identifier 20.1.1.1, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Dow
n   State/PfxRcd
20.1.1.2                 4   100    5          6       3      0      0  00:01:31
              0

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.0/24       0.0.0.0             0         100           32768    ?
*>   2.2.2.0/24       0.0.0.0             0         100           32768    ?
*>   3.3.3.0/24       0.0.0.0             0         100           32768    ?
*>   4.4.4.0/24       0.0.0.0             0         100           32768    ?
*>   5.5.5.0/24       0.0.0.0             0         100           32768    ?
*>   6.6.6.0/24       0.0.0.0             0         100           32768    ?

Total number of prefixes 6
#

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
S     1.1.1.0/24 [1/0] is directly connected, eth1, 00:06:54
S     2.2.2.0/24 [1/0] is directly connected, eth1, 00:06:35
S     3.3.3.0/24 [1/0] is directly connected, eth1, 00:06:26
S     4.4.4.0/24 [1/0] is directly connected, eth1, 00:06:17
S     5.5.5.0/24 [1/0] is directly connected, eth1, 00:06:09
S     6.6.6.0/24 [1/0] is directly connected, eth1, 00:06:01
C     20.1.1.0/24 is directly connected, eth1, 00:07:32
C     127.0.0.0/8 is directly connected, lo, 00:08:21
C     192.168.52.0/24 is directly connected, eth0, 00:08:17

Gateway of last resort is not set
#
```

R2

```
#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.0/24       0.0.0.0              0         100           32768    ?
*>   2.2.2.0/24       0.0.0.0              0         100           32768    ?
*>   3.3.3.0/24       0.0.0.0              0         100           32768    ?
*>   4.4.4.0/24       0.0.0.0              0         100           32768    ?
*>   5.5.5.0/24       0.0.0.0              0         100           32768    ?
*>   6.6.6.0/24       0.0.0.0              0         100           32768    ?

Total number of prefixes 6
#

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF “default”
B     1.1.1.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
B     2.2.2.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
```

```
B     3.3.3.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
B     4.4.4.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
B     5.5.5.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
B     6.6.6.0/24 [200/0] via 20.1.1.1, eth1, 00:13:44
C     20.1.1.0/24 is directly connected, eth1, 00:14:12
C     127.0.0.0/8 is directly connected, lo, 00:25:26
C     192.168.52.0/24 is directly connected, eth0, 00:25:23

Gateway of last resort is not set
#
```

R2

Now verify after applying table-map with filter option, only one route will be installed in FIB table according to route-map and access-list configured, BGP table remains same, table-map effect will be seen only for FIB table.

After applying table-map, clear BGP with “clear ip bgp table-map.”

```
(config)#router bgp 100
(config-router)#table-map test filter
(config-router)#end
#clear ip bgp table-map

#show ip bgp
BGP table version is 2, local router ID is 192.168.52.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.0/24       20.1.1.1              0         100           0        ?
*>i  2.2.2.0/24       20.1.1.1              0         100           0        ?
*>i  3.3.3.0/24       20.1.1.1              0         100           0        ?
*>i  4.4.4.0/24       20.1.1.1              0         100           0        ?
*>i  5.5.5.0/24       20.1.1.1              0         100           0        ?
*>i  6.6.6.0/24       20.1.1.1              0         100           0        ?

Total number of prefixes 6
#

#show ip bgp summary
BGP router identifier 192.168.52.5, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
20.1.1.1               4   100   40        39       2     0     0  00:18:33
6

Total number of neighbors 1
```



```
Total number of Established sessions 1
#

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     2.2.2.0/24 [200/0] via 20.1.1.1, eth1, 00:00:26
C     20.1.1.0/24 is directly connected, eth1, 00:19:01
C     127.0.0.0/8 is directly connected, lo, 00:30:15
C     192.168.52.0/24 is directly connected, eth0, 00:30:12

Gateway of last resort is not set
```

Table-map Without Filter Option

Remove filter option while applying table-map as below in R2

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Enter into BGP router mode
`(config-router)# table-map test`	Apply table-map with route-map created and with filter option
`(config-router)#end`	Exit from router and configure mode

```
#show running-config bgp
!
router bgp 100
 redistribute static
 neighbor 20.1.1.1 remote-as 100
 table-map test
!
#clear ip bgp table-map

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default
```

```
IP Route Table for VRF "default"
B     1.1.1.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
B     2.2.2.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
B     3.3.3.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
B     4.4.4.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
B     5.5.5.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
B     6.6.6.0/24 [200/0] via 20.1.1.1, eth1, 00:00:04
C     20.1.1.0/24 is directly connected, eth1, 00:31:16
C     127.0.0.0/8 is directly connected, lo, 00:42:30
C     192.168.52.0/24 is directly connected, eth0, 00:42:27

Gateway of last resort is not set
#
```

Note: Same can be tried with IPV6 VRF–v4 and VRF–v6 address-families and this feature is not supported for VPNV4 address-family

Route Target Constraint

BGP/MPLS IP VPNs use PE routers to Route Target (RT) extended communities and control the distribution of routes into the VRFs. Within a given iBGP mesh, PE routers hold routes marked with RouteTargets pertaining to VRFs that have local CE attachments.

BGP RT Constrained Route Distribution is a feature that can be used by service providers in Multiprotocol Label Switching (MPLS) Layer 3 VPNs to reduce the number of unnecessary routing updates that route reflectors (RRs) send to Provider Edge (PE) routers. The reduction in “routing updates” saves resources by allowing RRs, Autonomous System Boundary Routers (ASBRs), and PEs to carry fewer routes. Route targets are used to constrain routing updates.

With (MPLS)VPNs, the (iBGP) peers or Route Reflectors send all VPN4 and/or VPN6 prefixes to the PE routers. The PE routers drop the VPN4/6 prefixes for which there is no importing VPN route forwarding (VRF).

Topology

The topology below shows Route-target filtering in an L3VPN—with Route Target Constraint (RTC), the RR sends only wanted VPN4/6 prefixes to the PE; wanted” means that the PEs have the VRFs importing the specific prefixes.

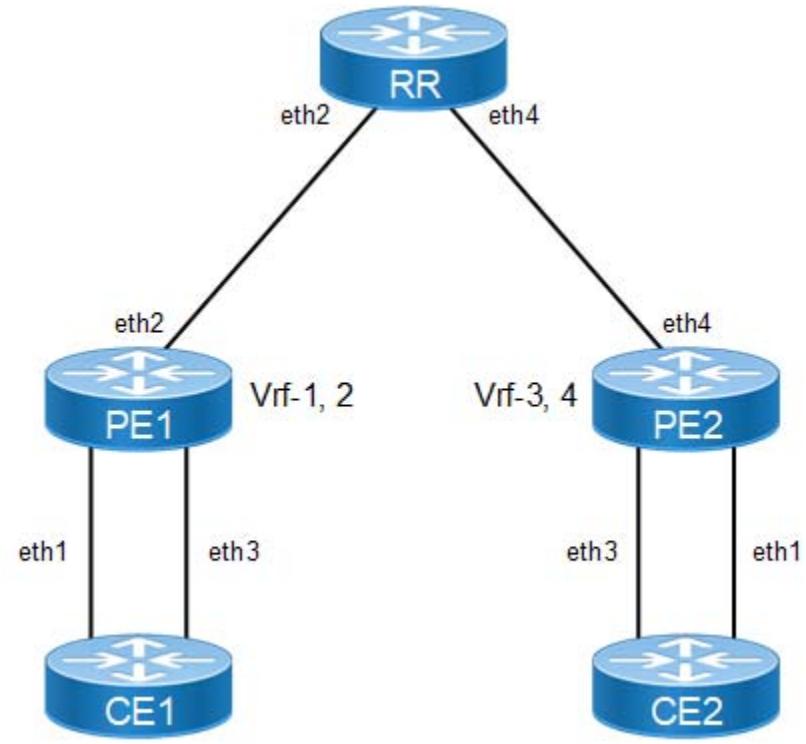


Figure 1-93: Route-target Filter Topology

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 80.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)#interface eth3`	Enter interface mode
`(config-if)#ip address 90.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)# router bgp 200`	Assign the ASN value (100) to the BGP router
`(config-router)#neighbor 80.1.1.2 remote-as 100` `(config-router)#neighbor 90.1.1.2 remote-as 100`	Configure neighbor (RR) in IBGP
`(config-router)#redistribute static`	Redistribute static routes into BGP
`(config-router)#exit`	Exit from router mode and enter configure mode
`(config)#ip route 1 1.1.1.0/24 eth1`	Configure static route with VRF 1 instance
`(config)#ip route 2 3.3.3.0/24 eth3`	Configure static route with VRF 2 instance
`(config)#ip route 2 4.4.4.0/24 eth3`	Configure static route with VRF 2 instance

CE2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 101.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)#interface eth3`	Enter interface mode
`(config-if)#ip address 100.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)# router bgp 200`	Assign the ASN value (100) to the BGP router
`(config-router)#neighbor 100.1.1.2 remote-as 100` `(config-router)#neighbor 101.1.1.2 remote-as 100`	Configure neighbor (RR) in IBGP
`(config-router)#end`	Exit from router and configure mode

PE1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf 1`	Create a VRF instance 1
`(config-vrf)#rd 1:100`	Configure unique RD value for VRF to identify VRF instance
`(config-vrf)#route-target export 1:200`	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
`(config-vrf)#exit`	Exit VRF mode and enter Configure mode
`(config)#ip vrf 2`	Create a VRF instance 2
`(config-vrf)#rd 1:300`	Configure unique RD value for VRF to identify VRF instance
`(config-vrf)#route-target both 1:400`	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
`(config-vrf)#exit`	Exit VRF mode and enter Configure mode
`(config)#router ldp`	Enable LDP.
`(config-router)#exit`	Exit router LDP mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure IP address for loopback interface
`(config-if)# enable-ldp ipv4`	Enable LDP on loopback interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding 1`	Bind interface to VRF 1
`(config-if)#ip address 80.1.1.2/24`	Configure IP address for VRF binded interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode

(config-if)#ip address 40.1.1.1/24	Configure an IP address for interface
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 2	Bind interface to VRF 1
(config-if)#ip address 90.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 11.11.11.11/32 area 0.0.0.0 (config-router)#network 40.1.1.0/24 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 22.22.22.22 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 22.22.22.22 update-source lo	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 22.22.22.22 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 22.22.22.22 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 1	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 80.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 80.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 2	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 90.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 90.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#end	Exit from router mode and configure mode

RR

(config)#router ldp	Enable LDP
(config-router)#exit	Exit router LDP mode

(config)#interface lo	Enter loopback interface
(config-if)#ip address 22.22.22.22/32 secondary (config-if)#ip address 44.44.44.44/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.2/24	Configure IP address for interface connecting to PE2
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#interface eth4	Enter into interface mode
(config-if)#ip address 50.1.1.1/24	Configure an IP address for interface connecting to PE1
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 22.22.22.22/32 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#network 40.1.1.0/24 area 0 (config-router)#network 44.44.44.44/32 area 0.0.0.0 (config-router)#network 50.1.1.0/24 area 0.0.0.0	Advertise PE1 to RR connected network in OSPF
(config-router)#exit	Exit from router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 11.11.11.11 remote-as 100	Configure neighbor (PE1) in IBGP
(config-router)#neighbor 11.11.11.11 update-source 22.22.22.22	Enable neighbor with loopback interface
(config-router)#neighbor 33.33.33.33 remote-as 100	Configure neighbor (PE2) in IBGP
(config-router)#neighbor 33.33.33.33 update-source 44.44.44.44	Enable neighbor with loopback interface
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor
(config-router-af)#neighbor 11.11.11.11 route-reflector-client	Configure PE1 as Route Reflector client
(config-router-af)#neighbor 33.33.33.33 route-reflector-client	Configure PE2 as Route Reflector client
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 route-reflector-client	Configure PE2 as Route Reflector client
(config-router-af)#neighbor 11.11.11.11 route-reflector-client	Configure PE1 as Route Reflector client
(config-router-af)#exit-address-family	Exit RTfilter Address-Family mode
(config-router)#end	Exit from Address-Family, Router and Configure mode.

PE2

#configure terminal	Enter configure mode.
(config)#ip vrf 3	Create a VRF instance 3
(config-vrf)#rd 1:600	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target export 1:200	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#ip vrf 4	Create a VRF instance 4
(config-vrf)#rd 1:900	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target both 1:400	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#router ldp	Enable LDP.
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface mode
(config-if)#ip address 33.33.33.33/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding 3	Bind interface to VRF 3
(config-if)#ip address 101.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 4	Bind interface to VRF 3
(config-if)#ip address 100.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#interface eth4	Enter interface mode
(config-if)#ip address 50.1.1.2/24	Configure an IP address for interface

(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE2 and RR
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE2 and RR
(config-router)#network 33.33.33.33/32 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#network 50.1.1.0/24 area 0	Advertise PE2 to RR connected network in OSPF
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 44.44.44.44 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 44.44.44.44 update-source 33.33.33.33	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 44.44.44.44 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 44.44.44.44 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 3	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 101.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 101.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 4	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 100.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 100.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#end	Exit router and configure mode

Validation

Through RTfilter address-family RT values will be exchanged between RR and PE’s. Neighbors are activated under this address-family and configured clients as well in this. RR will learn routes from PE’s and send to other PE’s if it has any peer requesting for that particular routes based on their RT import values

Below outputs shows the routes sent and learned in PE’s and installed in VRF’s and display’s RT filter values exchanged between them.

CE1

```
CE1#show ip bgp
BGP table version is 6, local router ID is 192.160.50.5
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.0/24       0.0.0.0             0         100            32768    ?
*>   3.3.3.0/24       0.0.0.0             0         100            32768    ?
*>   4.4.4.0/24       0.0.0.0             0         100            32768    ?

Total number of prefixes 3
```

PE1

```
PE1#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:100 (Default for VRF 1)
*>   1.1.1.0/24       80.1.1.1              0         100           0       200
?
*>   3.3.3.0/24       80.1.1.1              0         100           0       200
?
*>   4.4.4.0/24       80.1.1.1              0         100           0       200
?
 Announced routes count = 3
 Accepted routes count = 0
Route Distinguisher: 1:300 (Default for VRF 2)
*>   1.1.1.0/24       90.1.1.1              0         100           0       200
?
*>   3.3.3.0/24       90.1.1.1              0         100           0       200
?
*>   4.4.4.0/24       90.1.1.1              0         100           0       200
?
 Announced routes count = 3
 Accepted routes count = 0
PE1#


PE1#show ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 22.22.22.22
100:2:1:400
RTFilter's Sent
********************
peer-ip 22.22.22.22
100:2:1:400
PE1#
```

RR

```
RR#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300
*>i  1.1.1.0/24       11.11.11.11           0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11           0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11           0         100           0       200
?
 Announced routes count = 0
 Accepted routes count = 3
RR#


RR#show ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 11.11.11.11
100:2:1:400
peer-ip 33.33.33.33
100:2:1:400
RTFilter's Sent
********************
peer-ip 11.11.11.11
100:2:1:400
peer-ip 33.33.33.33
100:2:1:400
```

PE2

```
PE2#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300
*>i  1.1.1.0/24       11.11.11.11           0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11           0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11           0         100           0       200
?
 Announced routes count = 0
 Accepted routes count = 3
Route Distinguisher: 1:900 (Default for VRF 4)
*>i  1.1.1.0/24       11.11.11.11           0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11           0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11           0         100           0       200
?
```

```
 Announced routes count = 0
 Accepted routes count = 3
PE2#


PE2#show ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 44.44.44.44
100:2:1:400
RTFilter's Sent
********************
peer-ip 44.44.44.44
100:2:1:400
PE2#
```

BGP Labeled Unicast

As well as distributing routes, BGP with Multiprotocol Extensions (MP-BGP) can advertise MPLS label mappings that are mapped to routes. BGP Labeled Unicast (BGP-LU) attaches an MPLS label to an advertised IGP prefix and distributes the MPLS label mapped to the prefix to its peers.

With BGP-LU, a network can be divided into multiple regions to limit the total number of LSPs and enable failures to be contained and restored in a single region These regions operate separate instances of the IGP and use BGP-LU to advertise route information between inter-region routers.

A configuration for BGP-LU uses these type of nodes:

- Provider Edge (PE) nodes advertise label bindings to remote PEs in other regions. These advertisements only affect the PE routers and the ABRs and not provider routers (“P”) in the core network.
- Area Border Router (ABR) nodes advertise the label bindings to remote PEs in other regions.

BGP Labeled Unicast with LU as transport

Topology

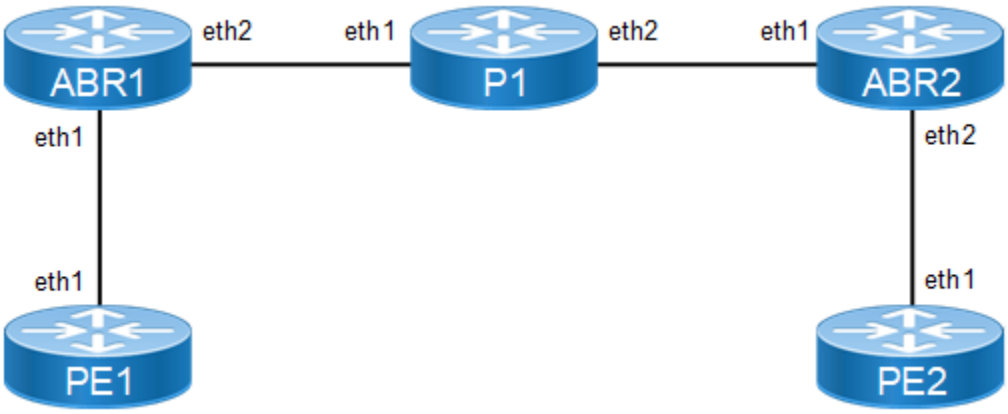


Figure 1-94: BGP labeled unicast

Configuration

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 11.11.11.55/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 172.4.5.55/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process OSPF with process Id 1
`(config-router)#network 172.4.5.0/24 area 0`	Define the interface (172.4.5.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 11.11.11.55/32 area 0`	Define the interface (11.11.11.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 21.21.21.56 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 21.21.21.56 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 172.4.5.52 remote-as 100`	Add neighbor with neighbor AS
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 172.4.5.52 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 21.21.21.56 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#network 11.11.11.55/32`	Advertise the loopback of RTR1 in BGP
`(config-router)#exit`	Exit from router BGP mode
`(config)# ip vrf vrf1`	Specify the name of the VRF (vrf1) to be created.
`(config-vrf)#rd 10:100`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 100:300`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.

(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 172.10.20.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

ABR1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 22.22.22.52/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.4.5.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 172.6.7.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.4.5.0/24 area 0	Define the interface (172.4.5.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.6.7.0/24 area 0	Define the interface (172.6.7.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 172.4.5.55 remote-as 100	Add neighbor with neighbor AS
(config-router)#neighbor 172.6.7.54 remote-as 100	Add neighbor with neighbor AS
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.6.7.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.4.5.55 activate	Activate the neighbor inside labeled-unicast address family

(config-router-af)# neighbor 172.4.5.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.4.5.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 200.200.200.54/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 172.1.2.54/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.6.7.54/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.1.2.0/24 area 0	Define the interface (172.1.2.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.6.7.0/24 area 0	Define the interface (172.6.7.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 172.1.2.55 remote-as 100	Add neighbor with neighbor AS
(config-router)#neighbor 172.6.7.54 remote-as 100	Add neighbor with neighbor AS
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.6.7.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.1.2.53 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 172.1.2.53 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

(config-router-af)# neighbor 172.6.7.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.1.2.53 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 44.44.44.53/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.1.2.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 172.3.4.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.1.2.0/24 area 0	Define the interface (172.1.2.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.3.4.0/24 area 0	Define the interface (172.3.4.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 172.1.2.55 remote-as 100	Add neighbor with neighbor AS
(config-router)#neighbor 172.3.4.54 remote-as 100	Add neighbor with neighbor AS
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.3.4.56 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.1.2.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 172.3.4.56 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.1.2.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

(config-router-af)# neighbor 172.3.4.56 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.1.2.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

PE2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 21.21.21.56/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 172.3.4.56/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.3.4.0/24 area 0	Define the interface (172.3.4.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 21.21.21.56/32 area 0	Define the interface (21.21.21.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 11.11.11.55 remote-as 100	Add loopback ip of PE1 as neighbor with neighbor AS
(config-router)#neighbor 11.11.11.55 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 172.3.4.52 remote-as 100	Add neighbor with neighbor AS
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.3.4.53 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#exit-address-family	Exit from address family IPv4 labeled unicast
(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
(config-router-af)#neighbor 11.11.11.55 activate	Activate the neighbor inside vpnv4 address family
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#network 21.21.21.56/32	Advertise the loopback of RTR1 in BGP
(config-router)#exit	Exit from router BGP mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.

(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 172.23.4.56/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

Validation

PE1

```
#show ip bgp neighbors 21.21.21.56
BGP neighbor is 21.21.21.56, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 11.11.11.55, remote router ID 21.21.21.56
  BGP state = Established, up for 00:00:38
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.55, Local port: 53175
Foreign host: 21.21.21.56, Foreign port: 179
Nexthop: 11.11.11.55
Nexthop global: ::
Nexthop local: ::
```

```
BGP connection: non shared network

#show ip bgp neighbors 172.4.5.52
BGP neighbor is 172.4.5.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 11.11.11.55, remote router ID 22.22.22.52
  BGP state = Established, up for 00:00:59
  Last read 00:00:30, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.55, Local port: 179
Foreign host: 172.4.5.52, Foreign port: 33889
Nexthop: 172.4.5.55
Nexthop global: 1121::55
Nexthop local: ::
BGP connection: non shared network

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>  11.11.11.55/32   0.0.0.0         24320          -
*>i 21.21.21.56/32    172.4.5.52         -            24321

#show mpls forwarding-table | include 21.21.21.56
   B>    21.21.21.56/32     1       0          Yes   LSP_DEFAULT    24321
eth1           172.4.5.52

#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, S - Stitched ILM

Code    FEC              ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf     Nexthop                        LSP-Type
   >  11.11.11.55/32    31         24320      N/A        N/A       N/A
127.0.0.1                    LSP_DEFAULT
```

```
#show mpls ftn-table
 Primary FTN entry with FEC: 21.21.21.56/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 1
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: BGP, out intf: eth1, out label: 24321
    Nexthop addr: 172.4.5.52        cross connect ix: 2, op code: Push
#show mpls vrf-table
Output for IPv4 VRF table with id: 2
 Primary FTN entry with FEC: 172.23.4.0/24, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 25, in intf: - in label: 0 out-segment ix: 24
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 24, owner: BGP, out intf: eth1, out label: 24321
    Nexthop addr: 21.21.21.56        cross connect ix: 25, op code: Push and
Lookup
```

ABR1

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
11.11.11.55     1   Full/Backup     00:00:39   172.4.5.55     eth1
0
200.200.200.54   1   Full/DR        00:00:39   172.6.7.54     eth2
0

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32    172.4.5.55      24320        24320
*>i 21.21.21.56/32    172.6.7.54      24321        24321

#show mpls forwarding-table | include 11.11.11.55
   B>    11.11.11.55/32     1       0          Yes   LSP_DEFAULT    24320
eth1          172.4.5.55
```

P1

```
#show ip bgp neighbors 172.6.7.52
BGP neighbor is 172.6.7.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 200.200.200.54, remote router ID 22.22.22.52
  BGP state = Established, up for 00:00:58
  Last read 00:00:29, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.6.7.54, Local port: 56703
Foreign host: 172.6.7.52, Foreign port: 179
Nexthop: 172.6.7.54
Nexthop global: 3323::54
Nexthop local: ::
BGP connection: non shared network

#show ip bgp neighbors 172.1.2.53
BGP neighbor is 172.1.2.53, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 200.200.200.54, remote router ID 44.44.44.53
  BGP state = Established, up for 00:00:58
  Last read 00:00:29, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.1.2.54, Local port: 179
Foreign host: 172.1.2.53, Foreign port: 48791
```

```
Nexthop: 172.1.2.54
Nexthop global: 4434::54
Nexthop local: ::
BGP connection: non shared network

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32    172.6.7.52      24320        24320
*>i 21.21.21.56/32    172.1.2.53      24321        24321

#show mpls forwarding-table | include 11.11.11.55
   B>    11.11.11.55/32     1       0          Yes   LSP_DEFAULT    24320
eth1           172.6.7.52
```

ABR2

```
#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32    172.1.2.54      24320        24320
*>i 21.21.21.56/32    172.3.4.56      24321        24320

#show mpls forwarding-table | include 11.11.11.55
   B>    11.11.11.55/32     1       0          Yes   LSP_DEFAULT    24320
eth1           172.1.2.54
```

PE2

```
#show ip bgp neighbors 11.11.11.55
BGP neighbor is 11.11.11.55, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 21.21.21.56, remote router ID 11.11.11.55
  BGP state = Established, up for 00:00:46
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
```

```
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 21.21.21.56, Local port: 179
Foreign host: 11.11.11.55, Foreign port: 53175
Nexthop: 21.21.21.56
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp neighbors 172.3.4.53
BGP neighbor is 172.3.4.53, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 21.21.21.56, remote router ID 44.44.44.53
  BGP state = Established, up for 00:01:01
  Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.56, Local port: 47822
Foreign host: 172.3.4.53, Foreign port: 179
Nexthop: 172.3.4.56
Nexthop global: 4435::56
Nexthop local: ::
BGP connection: non shared network

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32    172.3.4.53         -            24320
*>  21.21.21.56/32   0.0.0.0          24320           -

#show mpls forwarding-table | include 11.11.11.55
   B>    11.11.11.55/32     1       0          Yes   LSP_DEFAULT     24320
eth1          172.3.4.53
```

```
#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, S - Stitched ILM

Code    FEC              ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf     Nexthop                        LSP-Type
   >   21.21.21.56/32    185         24320       N/A         N/A        N/A
127.0.0.1                     LSP_DEFAULT

#show mpls ftn-table
 Primary FTN entry with FEC: 11.11.11.55/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 43, in intf: - in label: 0 out-segment ix: 42
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 42, owner: BGP, out intf: eth1, out label: 24320
    Nexthop addr: 172.3.4.53        cross connect ix: 43, op code: Push

#show mpls vrf-table
Output for IPv4 VRF table with id: 2
 Primary FTN entry with FEC: 172.10.20.0/24, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 49, in intf: - in label: 0 out-segment ix: 48
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 48, owner: BGP, out intf: eth1, out label: 24321
    Nexthop addr: 11.11.11.55        cross connect ix: 49, op code: Push and
Lookup
```

BGP Labeled Unicast with Seamless MPLS

Topology

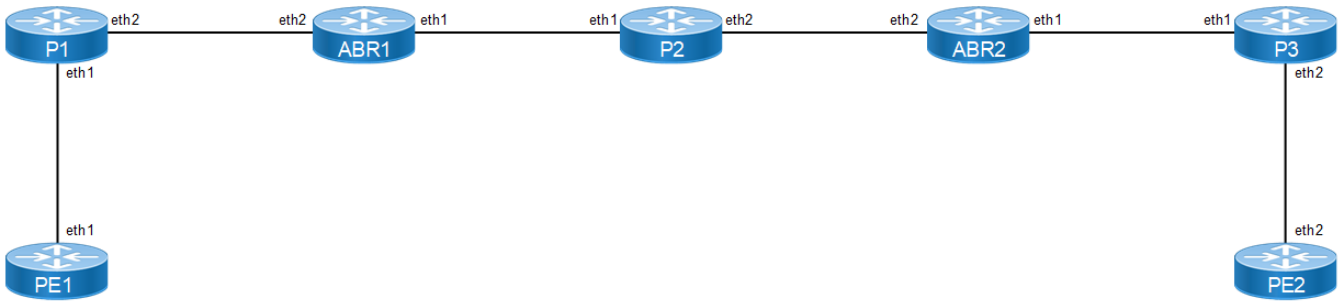


Figure 1-95: BGP_LU with MPLS

Configuration

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode

(config-if)#ip address 1.1.1.54/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.1.1.54/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 10
(config-router)#network 1.1.1.54/32 area 0	Define the interface (1.1.1.54/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 10.1.1.0/24 area 0	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 7.7.7.55 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 7.7.7.55 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 3.3.3.52 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 3.3.3.52 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 3.3.3.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#exit-address-family	Exit from address family IPv4 labeled unicast
(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
(config-router-af)#neighbor 7.7.7.55 activate	Activate the neighbor inside vpnv4 address family
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#network 1.1.1.54/32	Advertise the loopback of RTR1 in BGP
(config-router)#exit	Exit from router BGP mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 1.1.1.54 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.

(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 61.1.1.54/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.23/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.1.1.23/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.23/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 10
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24)) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 10.1.1.0/24 area 0	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 2.2.2.23/32 area 0	Define the interface (2.2.2.23/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 2.2.2.23 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 7.7.7.55/32 20.1.1.52	Specify the destination prefix and mask for the network and a gateway.
(config)# end	Exit from config mode

ABR1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.52/32`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 30.1.1.52/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 20.1.1.52/24`	Configure the IP address of the interface eth2
`(config-if)#label-switching`	Enable label-switching on interface eth2
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth2 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 20`	Configure the routing process OSPF with process id 20
`(config-router)#network 3.3.3.52/32 area 0`	Define the interface (3.3.3.52/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 20.1.1.0/24 area 0`	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)# router ldp`	Configure Router LDP instance
`(config-router)# transport-address ipv4 3.3.3.52 0`	Configure Transport address for LDP with label space value 0
`(config-router)#exit`	Exit from router mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 1.1.1.54 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 1.1.1.54 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 5.5.5.56 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 5.5.5.56 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 1.1.1.54 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#neighbor 5.5.5.56 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)# neighbor 1.1.1.54 route-reflector-client`	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

(config-router-af)# neighbor 5.5.5.56 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 1.1.1.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 5.5.5.56 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

P2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 4.4.4.53/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 30.1.1.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.53/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 20	Configure the routing process OSPF with process id 20
(config-router)#network 30.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 4.4.4.53/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 4.4.4.53 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode

(config-if)#ip address 5.5.5.56/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.56/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.56/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 5.5.5.56/32 area 0	Define the interface 5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router ospf 20	Configure the routing process OSPF with process id 20
(config-router)#network 5.5.5.56/32 area 0	Define the interface 5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 3.3.3.52 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 3.3.3.52 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 3.3.3.52 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 7.7.7.55 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 7.7.7.55 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 3.3.3.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 7.7.7.55 activate	Activate the neighbor inside labeled-unicast address family

(config-router-af)# neighbor 3.3.3.52 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 3.3.3.52 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

P3

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 6.6.6.22/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.22/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.22/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 50.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 60.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 6.6.6.22/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 6.6.6.22 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 1.1.1.54/32 50.1.1.56	Specify the destination prefix and mask for the network and a gateway.
(config)#exit	Exit from config mode

PE2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 7.7.7.55/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 60.1.1.55/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 30`	Configure the routing process OSPF with process id 10
`(config-router)#network 7.7.7.55/32 area 0`	Define the interface (7.7.7.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 1.1.1.54 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 1.1.1.54 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 5.5.5.56 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 5.5.5.56 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 5.5.5.56 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 1.1.1.54 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#network 7.7.7.55/32`	Advertise the loopback of RTR1 in BGP
`(config-router)#exit`	Exit from router BGP mode
`(config)# router ldp`	Configure Router LDP instance
`(config-router)# transport-address ipv4 7.7.7.55 0`	Configure Transport address for LDP with label space value 0
`(config-router)#exit`	Exit from router mode
`(config)# ip vrf vrf1`	Specify the name of the VRF (vrf1) to be created.

(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 62.1.1.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

Validation

PE1

```
#show ip bgp neighbors 3.3.3.52
BGP neighbor is 3.3.3.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 1.1.1.54, remote router ID 3.3.3.52
  BGP state = Established, up for 00:00:06
  Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 4 messages, 1 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 2; dropped 1
Local host: 1.1.1.54, Local port: 179
Foreign host: 3.3.3.52, Foreign port: 46745
Nexthop: 1.1.1.54
Nexthop global: 54::54
```

```
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:11, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show ip bgp neighbors 7.7.7.55
BGP neighbor is 7.7.7.55, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 1.1.1.54, remote router ID 7.7.7.55
  BGP state = Established, up for 00:01:10
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family VPNv4 Unicast: advertised and received
  Received 8 messages, 1 notifications, 0 in queue
  Sent 9 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: VPNv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 3; dropped 2
Local host: 1.1.1.54, Local port: 179
Foreign host: 7.7.7.55, Foreign port: 58871
Nexthop: 1.1.1.54
Nexthop global: 54::54
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:10, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)

#show mpls vrf-table
Output for IPv4 VRF table with id: 2
 Primary FTN entry with FEC: 62.1.1.0/24, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24961
    Nexthop addr: 7.7.7.55        cross connect ix: 12, op code: Push and
Lookup

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>  1.1.1.54/32      0.0.0.0         24961          -
*>i 7.7.7.55/32       3.3.3.52           -            24961

#show mpls forwarding-table | include 7.7.7.55
   B>    7.7.7.55/32        4       0          Yes   LSP_DEFAULT     24961
eth1          3.3.3.52
```

```
#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, S - Stitched ILM

Code    FEC              ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf     Nexthop                        LSP-Type
   >   1.1.1.54/32       11          24961      N/A         N/A        N/A
127.0.0.1                      LSP_DEFAULT
   >   61.1.1.0/24       13          24963      N/A         N/A        eth2
0.0.0.0                        LSP_DEFAULT

#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.23/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 10.1.1.23        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.52/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 24320
    Nexthop addr: 10.1.1.23        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 4, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: BGP, out intf: eth1, out label: 24961
    Nexthop addr: 3.3.3.52        cross connect ix: 4, op code: Push and
Lookup


 Primary FTN entry with FEC: 20.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 10.1.1.23        cross connect ix: 1, op code: Push
```

P1

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 10 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
1.1.1.54         1   Full/Backup    00:00:38   10.1.1.54      eth1
0
```

```
3.3.3.52        1   Full/DR        00:00:39    20.1.1.52      eth2
0
#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
1.1.1.54                  eth1       Active    OPERATIONAL   30    00:00:21
3.3.3.52                  eth2       Passive   OPERATIONAL   30    00:00:15
```

ABR1

```
#show ip bgp neighbors 1.1.1.54
BGP neighbor is 1.1.1.54, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 3.3.3.52, remote router ID 1.1.1.54
  BGP state = Established, up for 00:00:09
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x1
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 3.3.3.52, Local port: 46745
Foreign host: 1.1.1.54, Foreign port: 179
Nexthop: 3.3.3.52
Nexthop global: 52::52
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:14, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

#show ip bgp neighbors 5.5.5.56
BGP neighbor is 5.5.5.56, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 3.3.3.52, remote router ID 5.5.5.56
  BGP state = Established, up for 00:00:11
  Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
```

```
  Received 4 messages, 0 notifications, 0 in queue
  Sent 6 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 3, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 2; dropped 1
Local host: 3.3.3.52, Local port: 179
Foreign host: 5.5.5.56, Foreign port: 40440
Nexthop: 3.3.3.52
Nexthop global: 52::52
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:11, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       1.1.1.54        24960        24961
*>i 7.7.7.55/32       5.5.5.56        24961        24961

#show mpls forwarding-table | include 1.1.1.54
   L>    1.1.1.54/32        1       0          Yes   LSP_DEFAULT    24321
eth2          20.1.1.23
   B     1.1.1.54/32        7       0          Yes   LSP_DEFAULT    24961
eth2          1.1.1.54

#show mpls forwarding-table | include 7.7.7.55
   B>    7.7.7.55/32        8       0          Yes   LSP_DEFAULT    24961
eth1          5.5.5.56

#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 20.1.1.23        cross connect ix: 2, op code: Push
```

```
 Primary FTN entry with FEC: 1.1.1.54/32, id: 7, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24961
    Nexthop addr: 1.1.1.54        cross connect ix: 11, op code: Push and
Lookup


 Primary FTN entry with FEC: 2.2.2.23/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 4.4.4.53/32, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 30.1.1.53        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 5.5.5.56/32, id: 5, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 9
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 9, owner: LDP, out intf: eth1, out label: 24320
    Nexthop addr: 30.1.1.53        cross connect ix: 10, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 8, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24961
    Nexthop addr: 5.5.5.56        cross connect ix: 12, op code: Push and
Lookup


 Primary FTN entry with FEC: 10.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 5, op code: Push
```

```
 Primary FTN entry with FEC: 40.1.1.0/24, id: 6, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 30.1.1.53        cross connect ix: 7, op code: Push
```

P2

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 20 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address         Interface
Instance ID
3.3.3.52         1   Full/Backup     00:00:39    30.1.1.52      eth1
0
5.5.5.56         1   Full/DR         00:00:40    40.1.1.56      eth2
0

#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
3.3.3.52                  eth1       Active    OPERATIONAL   30    00:00:21
5.5.5.56                  eth2       Passive   OPERATIONAL   30    00:00:19
```

ABR2

```
#show ip bgp neighbors 3.3.3.52
BGP neighbor is 3.3.3.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 5.5.5.56, remote router ID 3.3.3.52
  BGP state = Established, up for 00:00:12
  Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 5 messages, 1 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x1
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes
```

```
 Connections established 2; dropped 1
Local host: 5.5.5.56, Local port: 40440
Foreign host: 3.3.3.52, Foreign port: 179
Nexthop: 5.5.5.56
Nexthop global: 56::56
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:17, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show ip bgp neighbors 7.7.7.55
BGP neighbor is 7.7.7.55, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 5.5.5.56, remote router ID 7.7.7.55
  BGP state = Established, up for 00:00:13
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.56, Local port: 35004
Foreign host: 7.7.7.55, Foreign port: 179
Nexthop: 5.5.5.56
Nexthop global: 56::56
Nexthop local: ::
BGP connection: non shared network

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32      3.3.3.52        24960        24960
*>i 7.7.7.55/32      7.7.7.55        24961        24960

#show mpls forwarding-table | include 1.1.1.54
```



```
   B>    1.1.1.54/32        7       0          Yes   LSP_DEFAULT     24960
eth2           3.3.3.52

#show mpls forwarding-table | include 7.7.7.55
   L>    7.7.7.55/32        5       0          Yes   LSP_DEFAULT     24320
eth1           50.1.1.22
   B     7.7.7.55/32        8       0          Yes   LSP_DEFAULT     24960
eth1           7.7.7.55

#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 7, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24960
    Nexthop addr: 3.3.3.52        cross connect ix: 11, op code: Push and
Lookup


 Primary FTN entry with FEC: 3.3.3.52/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 40.1.1.53        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 4.4.4.53/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 40.1.1.53        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 5, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 9
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 9, owner: LDP, out intf: eth1, out label: 24320
    Nexthop addr: 50.1.1.22        cross connect ix: 10, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 8, row status: Active
```

```
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24960
    Nexthop addr: 7.7.7.55        cross connect ix: 12, op code: Push and
Lookup


 Primary FTN entry with FEC: 30.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 40.1.1.53        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 60.1.1.0/24, id: 6, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 7, op code: Push
```

P3

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 30 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
5.5.5.56          1   Full/Backup     00:00:39    50.1.1.56       eth1
0
7.7.7.55          1   Full/DR         00:00:39    60.1.1.55       eth2
0

#show ldp session
Peer IP Address          IF Name    My Role    State       KeepAlive  UpTime
5.5.5.56                 eth1        Active    OPERATIONAL   30    00:00:30
7.7.7.55                 eth2       Passive   OPERATIONAL   30    00:00:28
```

PE2

```
#show ip bgp neighbors 5.5.5.56
BGP neighbor is 5.5.5.56, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 7.7.7.55, remote router ID 5.5.5.56
  BGP state = Established, up for 00:00:16
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 MPLS LABEL: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
```

```
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 For address family: IPv4 Labeled MPLS
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 7.7.7.55, Local port: 179
Foreign host: 5.5.5.56, Foreign port: 35004
Nexthop: 7.7.7.55
Nexthop global: 55::55
Nexthop local: ::
BGP connection: non shared network

#show mpls vrf-table
Output for IPv4 VRF table with id: 2
 Primary FTN entry with FEC: 61.1.1.0/24, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24963
    Nexthop addr: 1.1.1.54        cross connect ix: 11, op code: Push and
Lookup

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       5.5.5.56           -            24960
*>  7.7.7.55/32      0.0.0.0         24960          -

#show mpls forwarding-table | include 1.1.1.54
   B>    1.1.1.54/32        4       0          Yes   LSP_DEFAULT    24960
eth2          5.5.5.56

#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
       K - CLI ILM, T - MPLS-TP, S - Stitched ILM

Code    FEC              ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf     Nexthop                        LSP-Type
   >   7.7.7.55/32       9          24960      N/A        N/A        N/A
127.0.0.1                     LSP_DEFAULT
   >   62.1.1.0/24       10         24961      N/A        N/A        eth1
0.0.0.0                       LSP_DEFAULT

#show mpls ftn-table
```

```
 Primary FTN entry with FEC: 1.1.1.54/32, id: 4, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: BGP, out intf: eth2, out label: 24960
    Nexthop addr: 5.5.5.56        cross connect ix: 4, op code: Push and
Lookup


 Primary FTN entry with FEC: 5.5.5.56/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 60.1.1.22        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 60.1.1.22        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 50.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 60.1.1.22        cross connect ix: 2, op code: Push
```

BGP Labeled Unicast with Inter-AS

Topology

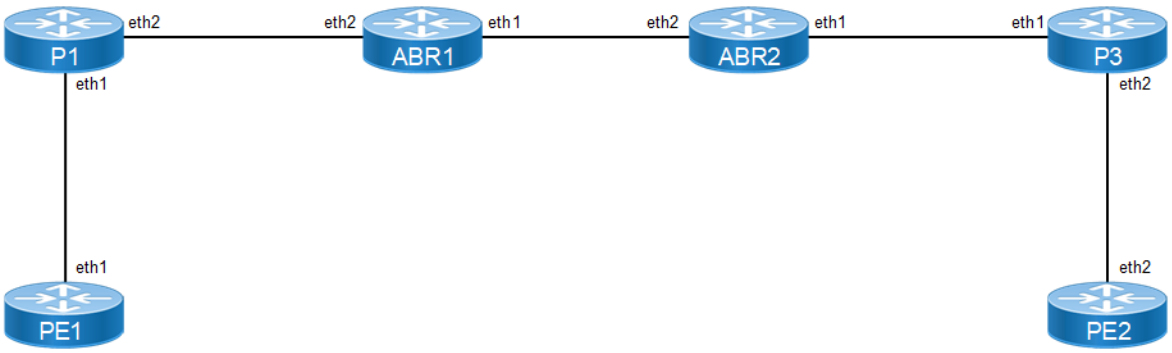


Figure 1-96: BGP Labeled unicast with Inter-AS

Configurations

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.54/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.1.1.54/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure the routing process OSPF with process id 10
`(config-router)#network 1.1.1.54/32 area 0`	Define the interface (1.1.1.54/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 10.1.1.0/24 area 0`	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 7.7.7.55 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 7.7.7.55 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 3.3.3.52 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 3.3.3.52 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 3.3.3.52 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 7.7.7.55 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#network 1.1.1.54/32`	Advertise the loopback of RTR1 in BGP
`(config-router)#exit`	Exit from router BGP mode
`(config)# router ldp`	Configure Router LDP instance
`(config-router)# transport-address ipv4 1.1.1.54 0`	Configure Transport address for LDP with label space value 0
`(config-router)#exit`	Exit from router mode

(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 61.1.1.54/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.23/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.1.1.23/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.23/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 10
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24)) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 10.1.1.0/24 area 0	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 2.2.2.23/32 area 0	Define the interface (2.2.2.23/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance

(config-router)# transport-address ipv4 2.2.2.23 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 7.7.7.55/32 20.1.1.52	Specify the destination prefix and mask for the network and a gateway.
(config)# end	Exit from config mode

ABR1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 3.3.3.52/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 52.56.1.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.52/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 20
(config-router)#network 3.3.3.52/32 area 0	Define the interface (3.3.3.52/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 3.3.3.52 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 1.1.1.54 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 1.1.1.54 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 52.56.1.56 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family

(config-router-af)#neighbor 1.1.1.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 52.56.1.56 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 1.1.1.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 1.1.1.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 52.56.1.56 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 5.5.5.56/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.56/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 52.56.1.56/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process Id 1
(config-router)#network 5.5.5.56/32 area 0	Define the interface (5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 5.5.5.56 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)#router bgp 200	Enter Router BGP mode
(config-router)#neighbor 52.56.1.52 remote-as 100	Add neighbor peer ip and neighbor AS
(config-router)#neighbor 7.7.7.55 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 7.7.7.55 update-source lo	Update the source for that particular neighbor as loopback interface

(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 52.56.1.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 7.7.7.55 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 7.7.7.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 52.56.1.52 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

P2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 6.6.6.22/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.22/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.22/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 50.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 60.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 6.6.6.22/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 6.6.6.22 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode

(config)# ip route 1.1.1.54/32 50.1.1.56	Specify the destination prefix and mask for the network and a gateway.
(config)#exit	Exit from Cofig mode

PE2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 7.7.7.55/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.55/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process id 10
(config-router)#network 7.7.7.55/32 area 0	Define the interface (7.7.7.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 60.1.1.0/24 area 0	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 200	Enter Router BGP mode
(config-router)#neighbor 1.1.1.54 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 1.1.1.54 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 1.1.1.54 ebgp-multihop	Enable neighbor connection between two eBGP
(config-router)#neighbor 5.5.5.56 remote-as 200	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 5.5.5.56 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 5.5.5.56 activate	Activate the neighbor inside vpnv4 address family
(config-router-af)#exit-address-family	Exit from address family IPv4 labeled unicast
(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
(config-router-af)#neighbor 1.1.1.54 allow-ebgp-vpn	Allow eBGP neighbor to be a vpn peer.
(config-router-af)#neighbor 1.1.1.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#network 7.7.7.55/32	Advertise the loopback of RTR1 in BGP

(config-router)#exit	Exit from router BGP mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 7.7.7.55 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 62.1.1.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

Validation

PE1

```
#sh ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>  1.1.1.54/32      0.0.0.0         24969          -
*>i 7.7.7.55/32       3.3.3.52           -            24322

#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
   L>    2.2.2.23/32          1       0          Yes   LSP_DEFAULT     3
eth1          10.1.1.23
   L>    3.3.3.52/32          3       0          Yes   LSP_DEFAULT     24321
eth1          10.1.1.23
   B>    7.7.7.55/32          4       0          Yes   LSP_DEFAULT     24322
eth1          3.3.3.52
   L>    20.1.1.0/24          2       0          Yes   LSP_DEFAULT     3
eth1          10.1.1.23

#sh mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.23/32, id: 1, row status: Active
```

```
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 10.1.1.23        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.52/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 24321
    Nexthop addr: 10.1.1.23        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 4, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: BGP, out intf: eth1, out label: 24322
    Nexthop addr: 3.3.3.52        cross connect ix: 4, op code: Push and
Lookup


 Primary FTN entry with FEC: 20.1.1.0/24, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 10.1.1.23        cross connect ix: 1, op code: Push
```

ABR1

```
#sh ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       1.1.1.54        24323        24969
*>  7.7.7.55/32       52.56.1.56      24322        24325

#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
   L>   1.1.1.54/32        2       0          Yes   LSP_DEFAULT     24322
eth2          20.1.1.23
   B    1.1.1.54/32        5       0          Yes   LSP_DEFAULT     24969
eth2          1.1.1.54
   L>   2.2.2.23/32        3       0          Yes   LSP_DEFAULT     3
eth2          20.1.1.23
```

```
   B>    7.7.7.55/32        1       0          Yes   LSP_DEFAULT     24325
eth1          52.56.1.56
   L>    10.1.1.0/24        4       0          Yes   LSP_DEFAULT     3
eth2          20.1.1.23

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 24322
    Nexthop addr: 20.1.1.23        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 1.1.1.54/32, id: 5, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 8
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 8, owner: BGP, out intf: eth2, out label: 24969
    Nexthop addr: 1.1.1.54        cross connect ix: 8, op code: Push and
Lookup


 Primary FTN entry with FEC: 2.2.2.23/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 7
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 7, owner: BGP, out intf: eth1, out label: 24325
    Nexthop addr: 52.56.1.56        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 10.1.1.0/24, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 3, op code: Push
```

ABR2

```
#sh ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
```

```
*>  1.1.1.54/32       52.56.1.52      24322        24323
*>i 7.7.7.55/32       7.7.7.55        24325        24967

#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
   B>   1.1.1.54/32         1       0          Yes   LSP_DEFAULT     24323
eth2          52.56.1.52
   L>   6.6.6.22/32         2       0          Yes   LSP_DEFAULT     3
eth1          50.1.1.22
   L>   7.7.7.55/32         3       0          Yes   LSP_DEFAULT     24322
eth1          50.1.1.22
   B    7.7.7.55/32         5       0          Yes   LSP_DEFAULT     24967
eth1          7.7.7.55
   L>   60.1.1.0/24         4       0          Yes   LSP_DEFAULT     3
eth1          50.1.1.22

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 8
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 8, owner: BGP, out intf: eth2, out label: 24323
    Nexthop addr: 52.56.1.52        cross connect ix: 8, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth1, out label: 24322
    Nexthop addr: 50.1.1.22        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 5, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 7
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 7, owner: BGP, out intf: eth1, out label: 24967
    Nexthop addr: 7.7.7.55        cross connect ix: 7, op code: Push and
Lookup
```

```
 Primary FTN entry with FEC: 60.1.1.0/24, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 2, op code: Push
```

PE2

```
#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
    Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       5.5.5.56           -            24322
*>  7.7.7.55/32      0.0.0.0         24967          -

#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
      B - BGP FTN, K - CLI FTN, t - tunnel
      L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
      U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
  B>    1.1.1.54/32        4       0          Yes   LSP_DEFAULT     24322
eth2          5.5.5.56
  L>    5.5.5.56/32        3       0          Yes   LSP_DEFAULT     24321
eth2          60.1.1.22
  L>    6.6.6.22/32        2       0          Yes   LSP_DEFAULT     3
eth2          60.1.1.22
  L>    50.1.1.0/24        1       0          Yes   LSP_DEFAULT     3
eth2          60.1.1.22

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 4, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 36, in intf: - in label: 0 out-segment ix: 37
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 37, owner: BGP, out intf: eth2, out label: 24322
    Nexthop addr: 5.5.5.56        cross connect ix: 36, op code: Push and
Lookup


 Primary FTN entry with FEC: 5.5.5.56/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 60.1.1.22        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
```

```
 Tunnel id: 0,   Protected LSP id: 0, Description: N/A
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 8
     Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 8, owner: LDP, out intf: eth2, out label: 3
   Nexthop addr: 60.1.1.22        cross connect ix: 9, op code: Push


Primary FTN entry with FEC: 50.1.1.0/24, id: 1, row status: Active
 Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0,   Protected LSP id: 0, Description: N/A
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 8
     Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 8, owner: LDP, out intf: eth2, out label: 3
   Nexthop addr: 60.1.1.22        cross connect ix: 9, op code: Push
```

BGP Best Path Selection Process

BGP assigns the first valid path as the current best path. BGP then compares the best path with the next path in the list, until BGP reaches the end of the list of valid paths. Below steps provides the rules that are used to determine the best path:

1. Prefer the path with the highest WEIGHT.
2. Prefer the path with the highest LOCAL_PREF.
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand or through redistribution from an IGP.
4. Prefer the path with the shortest AS_PATH.

Note: Beware of these items:

- This step is skipped if user has configured the `bgp bestpath as-path ignore` command.
- If `bgp bestpath compare-confed-aspath` is configured then Prefer the path with the shortest AS_CONFED path.

5. Prefer the path with the lowest ORIGIN type.

Note: Beware of below listed items:

- IGP is lower than Exterior Gateway Protocol (EGP), and EGP is lower than INCOMPLETE.

6. Prefer the path with the lowest multi-exit discriminator (MED).

Note: Beware of these items:

- By default, MED is compared in these cases:
  - MEDs are compared only if the first AS in the AS_SEQUENCE is the same for multiple paths
  - If both the paths are internal as routes
  - If paths have confederation as-path then MEDs are compared only if the first AS in the BGP_AS_CONFED_SEQUENCE is the same for multiple paths
  - To override all above checks, user can configure `bgp always-compare-med` command

7. Prefer eBGP over iBGP paths.

Note: Beware of below listed item:

- EBGP is preferred over IGBP or EBGP is preferred over CONFED.

8. Path learned from LU Address-family is preferred over IPv4 Unicast Address-family.

Note: Beware of these items:

- This is Exception Rule for IPv4 Labeled-Unicast Address-family.
- This rule applicable only for IPv4 Labeled-Unicast/Unicast routes over default VRF.

9. Prefer the path with the lowest IGP metric to the BGP next hop.
10. Determine if multiple paths require installation in the routing table for BGP Multipath and mark the ECMP candidate.
11. When both paths are external, prefer the path that was received first (the oldest one). This step minimizes route-flap, since a newer path won't displace an older one, even if it was the preferred route based on the additional decision criteria below. This has to be enabled by BGP command `bestpath tie-break-on-age`

Note: Beware of these items:

- Skip this step if any of these items are true:
  - If `bgp bestpath compare-routerid` is configured in addition to `bestpath tie-break-on-age`, then this step will be skipped.
  - If the router ID is same for multiple paths, because the routes were received from the same router, then this step will be skipped.

12. Router ID and Originator Id:
    - If `bgp bestpath compare-routerid` is configured, then prefer the route that comes from the BGP router with the lowest Router ID.
    - If `bgp bestpath dont-compare-originator-id` is not configured, prefer the route that comes from the BGP router with the lowest Router ID.

Note: Beware of the below listed item:

- If a path contains Route Reflector (RR) attributes, the Originator ID is substituted for the Router ID in the path selection process.
- If `bgp bestpath dont-compare-originator-id` is configured, prefer the route that comes from the BGP router with the lowest router ID. In this case, Originator ID is not compared even if the RR attribute is present.

13. If the originator or Router ID is the same for multiple paths, prefer the path with the minimum cluster list length.

Prefer the path that comes from the lowest neighbor address.

BGP Dampening

BGP supports route dampening for IPv4 and IPv6 prefixes. Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit, the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is unsuppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

Topology

In this example, a successful TCP connection is being established between the routers.

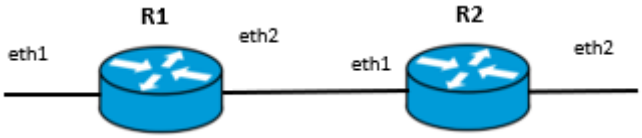


Figure 1-97: BGP dampening

IPv4 Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 1.1.1.1 secondary`	Configure the secondary loopback address
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 101.1.0.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 100`	Configure BGP with the AS number 100
`(config-router)#neighbor 10.1.1.2 remote-as 200`	Define the BGP neighbor, and establish a TCP session. 10.1.1.2 is the IP address of one of the neighbors (R2), and 200 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 100.1.0.2 is the IP address of one of the neighbors on interface eth1, and 300 is the neighbor's AS number.
`(config-router)#redistribute connected`	Enable redistribute connected
`(config-router)#exit`	Exit router configure mode

R2

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 2.2.2.2 secondary`	Configure the secondary loopback address
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 101.1.0.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Configure BGP with the AS number 100

`(config-router)#redistribute connected`	Enable redistribute connected
`(config-router)#bgp dampening`	Enable BGP dampening with default values: • Reachability half-life is 15 minutes • Reuse limit is 750: • Suppress limit is 2000 • Max-suppress value is 60 minutes • Un-reachability half-life is 15 minutes
`(config-router)#neighbor 10.1.1.1 remote-as 100`	Define the BGP neighbor, and establish a TCP session. 10.1.1.1 is the IP address of one of the neighbors (R1), and 100 is the neighbor's AS number.
`(config-router)#neighbor 101.1.0.2 remote-as 400`	Define the BGP neighbor, and establish a TCP session. 101.1.0.2 is the IP address of one of the neighbors on eth2 interface, and 400 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 100.1.0.2 is the IP address of one of the neighbors of router R1 on eth1 interface, and 300 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 ebgp-multihop 2`	Increase BGP neighbors with ebgp-multihop value

Validation

R2

Verify the BGP dampening parameters.

```
#sh ip bgp dampening parameters

 dampening 15 750 2000 60 15
 Dampening Control Block(s):
  Reachability Half-Life time    : 15 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reachability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
```

Verify BGP dampened paths for flapping networks.

```
#sh ip bgp dampening dampened-paths
BGP table version is 21, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                Reuse   Path
 d   200.1.0.0        10.1.1.1             00:29:00 100 300 i
 d   200.2.0.0        10.1.1.1             00:28:20 100 300 i
 d   200.3.0.0        10.1.1.1             00:28:20 100 300 i
 d   200.4.0.0        10.1.1.1             00:28:20 100 300 i
 d   200.5.0.0        10.1.1.1             00:28:20 100 300 i
 d   200.6.0.0        10.1.1.1             00:28:20 100 300 i
 d   200.7.0.0        10.1.1.1             00:28:20 100 300 i
```

```
 d   200.8.0.0        10.1.1.1              00:28:20 100 300 i
 d   200.9.0.0        10.1.1.1              00:28:20 100 300 i
 d   200.10.0.0       10.1.1.1              00:28:20 100 300 i
```

Verify BGP dampening flap statistics for flapping networks.

```
#sh ip bgp dampening flap-statistics
BGP table version is 21, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                Flaps  Duration  Reuse   Path
 d   200.1.0.0        10.1.1.1                8  00:18:37  00:29:10  100 300 i
 d   200.2.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.3.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.4.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.5.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.6.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.7.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.8.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.9.0.0        10.1.1.1                7  00:14:22  00:29:00  100 300 i
 d   200.10.0.0       10.1.1.1                7  00:14:22  00:29:00  100 300 i
```

IPv6 Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 2000:0:0:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 2000:0:2:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 100`	Configure BGP with the AS number 100
`(config-router)#neighbor 2000:0:0:1::2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 2000:0:0:1::2 is the IP address of one of the neighbors on interface eth1, and 300 is the neighbor's AS number.
`(config-router)#neighbor 2000:0:2:1::2 remote-as 200`	Define the BGP neighbor, and establish a TCP session. 2000:0:2:1::2 is the IP address of one of the neighbors (R2), and 200 is the neighbor's AS number.
`(config-router)#redistribute connected`	Enable redistribute connected
`(config-router)#address-family ipv6 unicast`	Enter IPv6 address family
`(config-router-af)neighbor 2000:0:0:1::2 activate`	Activate BGP neighbor
`(config-router-af)neighbor 2000:0:2:1::2 activate`	Activate BGP neighbor

R2

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 2000:0:2:1::2/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 2000:0:1:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Configure BGP with the AS number 200
`(config-router)#redistribute connected`	Enable redistribute connected
`(config-router)#neighbor 2000:0:1:1::2 remote-as 400`	Define the BGP neighbor, and establish a TCP session. 2000:0:1:1::2 is the IP address of one of the neighbors on interface eth2, and 400 is the neighbor's AS number.
`(config-router)#neighbor 2000:0:2:1::1 remote-as 100`	Define the BGP neighbor, and establish a TCP session. 2000:0:2:1::1 is the IP address of one of the neighbors (R1), and 100 is the neighbor's AS number.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 address-family
`(config-router-af)#bgp dampening`	Enable BGP dampening with default values: • Reachability half-life is 15 minutes • Reuse limit is 750 • Suppress limit is 2000 • Max-suppress value is 60 minutes • Un-reachability half-life is 15 minutes
`(config-router-af)#neighbor 2000:0:1:1::2 activate`	Activate BGP neighbor
`(config-router-af)#neighbor 2000:0:2:1::1 activate`	Activate BGP neighbor

Validation

R2

Verify the IPv6 BGP dampening parameters.

```
#sh bgp dampening parameters

 dampening 15 750 2000 60 15
 Dampening Control Block(s):
  Reachability Half-Life time    : 15 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reachability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
```

Verify IPv6 BGP dampened paths for flapping networks.

```
#sh bgp dampening dampened-paths
```

```
BGP table version is 7, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                  Reuse   Path
*d   3000:0:1:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:2:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:3:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:4:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:5:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:6:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:7:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:8:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:9:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
*d   3000:0:a:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                   00:18:30 100 300 i
```

Verify IPv6 BGP dampening flap statistics for flapping networks.

```
#sh bgp dampening flap-statistics
BGP table version is 7, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                Flaps  Duration  Reuse   Path
*d   3000:0:1:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:2:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:3:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:4:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:5:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:6:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:7:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
*d   3000:0:8:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                            4  00:05:19  00:18:30  100 300 i
```

```
*d   3000:0:9:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    4  00:05:19  00:18:30  100 300 i
*d   3000:0:a:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    4  00:05:19  00:18:30  100 300 i
```

CHAPTER 2 BGP4+

This chapter contains basic BGP4+ configuration examples.

For details about the commands used in these examples, see the *Border Gateway Protocol Command Reference*.

Enable iBGP Peering Using a Global Address

This example shows the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same Autonomous System (AS), AS200, connecting to network 3ffe:10::/48. First, specify the IPv6 global address, then define the routing process and AS number to which the routers belong. Configure a fixed Router ID, then, define BGP neighbors to start exchanging routing updates.

Topology

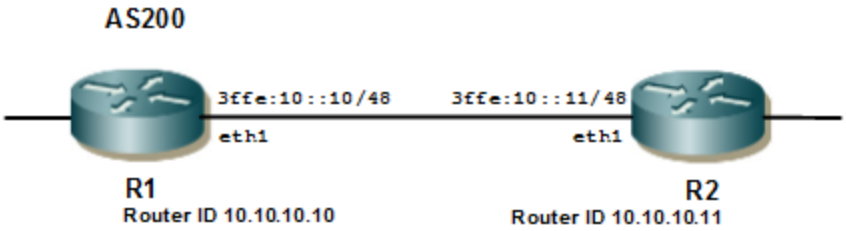


Figure 2-98: iBGP Peering

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure.
`(config-if)#ipv6 address 3ffe:10::10/48`	Specify the IPv6 global address.
`(config-if)#exit`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R1`.
`(config-router)#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::11 remote-as 200`	Define BGP neighbor `R2`, and establish a TCP session by specifying the global IPv6 address (`3ffe:10::11`) and the AS number (`200`) of neighbor R2.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::11 activate`	Activate the neighbor `R2(3ffe:10::11)`, and enable exchange of IPv6 address prefix types with this neighbor.

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to configure.
`(config-if)#ipv6 address 3ffe:10::11/48`	Specify the IPv6 global address.
`(config-if)#exit`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R2.
`(config-router)#bgp router-id 10.10.10.11`	Configure a fixed Router ID (`10.10.10.11`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::10 remote-as 200`	Define the BGP neighbor (R1), and establish a TCP session by specifying the global IPv6 address (`3ffe:10::10`)and the AS number`(200)`of neighbor `R1`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::10 activate`	Activate the neighbor `R1(3ffe:10::10)`, and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Enable iBGP Peering Using Link-local Address

This example shows the minimum configuration required to enable iBGP on an interface. R1 and R2 are two routers belonging to the same AS, AS200, connecting to network fe80::/10. First, define the routing process and AS number to which the routers belong. Configure a fixed Router ID for the BGP4+ routing process, then, define BGP neighbors to start exchanging routing updates.

Topology

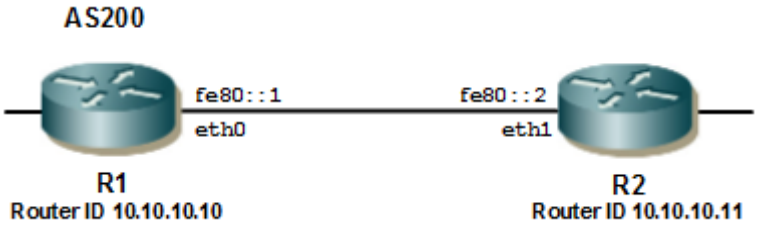


Figure 2-99: iBGP Peering Link-Local Address

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R1`.
`(config-router)#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor fe80::2 remote-as 200`	Define BGP neighbor (R2), and establish a TCP session by specifying the link-local address (`fe80::2`) and the AS number (`200`) of neighbor `R2`.
`(config-router)#neighbor fe80::2 interface eth0`	To specify a link-local neighbor, configure the interface name of the neighbor `fe80::2`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor fe80::2 activate`	Activate the neighbor `R2(fe80::2)`, and enable exchange of IPv6 address prefix types with this neighbor.

R2

`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R2`.
`(config-router)#bgp router-id 10.10.10.11`	Configure a fixed Router ID (`10.10.10.11`) for the BGP4+ routing process.
`(config-router)#neighbor fe80::1 remote-as 200`	Define the BGP neighbor (R1), and establish a TCP session by specifying the link-local address `R1(fe80::1)` and the AS number (`200`) of neighbor `R1`.
`(config-router)#neighbor fe80::1 interface eth1`	To specify a link-local neighbor, configure the interface name of the neighbor `fe80::1`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor fe80::1 activate`	Activate the neighbor `R1(fe80:1)`, and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6, show bgp ipv6 neighbors

Enable eBGP Peering Between Different Autonomous Systems

This example shows the minimum configuration required to enable eBGP on an interface, when the routers belong to different ASs. R1 and R2 are two routers in different ASs, AS200 and AS300 connecting to network 3ffe:10::/64.

Topology

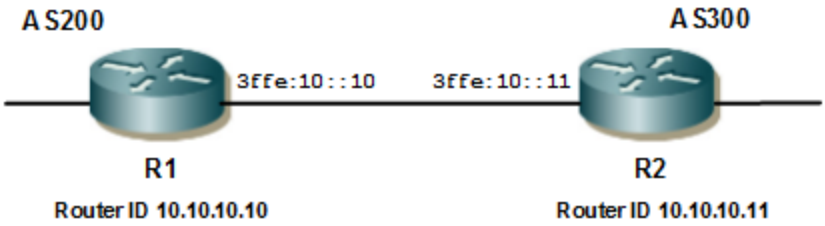


Figure 2-100: BGP Peering - Different AS

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)``#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)``#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)``#neighbor 3ffe:10::11 remote-as 300`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::11`) and the AS number (`300`) of neighbor R2.
`(config-router)``#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)``#neighbor 3ffe:10::11 activate`	Activate the neighbor R2 (`3ffe:10::11`), and enable exchange of IPv6 address prefix types with this neighbor.

R2

`(config)``#router bgp 300`	Define the routing process. The number `300` specifies the AS number of R2.
`(config-router)``#bgp router-id 10.10.10.11`	Configure a fixed Router ID (`10.10.10.11`) for the BGP4+ routing process.
`(config-router)``#neighbor 3ffe:10::10 remote-as 200`	Define the BGP neighbor (R1), and establish a TCP session by specifying the IPv6 address (`3ffe:10::10`) and the AS number (`200`) of neighbor R1.
`(config-router)``#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)``#neighbor 3ffe:10::10 activate`	Activate the neighbor R1 (`3ffe:10::10`) and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Route-Map

Use route-maps to filter incoming updates from a BGP peer. In this example, a prefix list named `myPrefixList` on R1 is configured to deny entry of any routes with the IP address 3ffe:12::/32. To test the filter, R2 is configured to generate network prefixes 3ffe:11::/48 and 3ffe:12::/48. To verify, use the `show bgp ipv6` command on R1; it displays R1 receiving only the 3ffe:11::/48 network prefix.

Topology

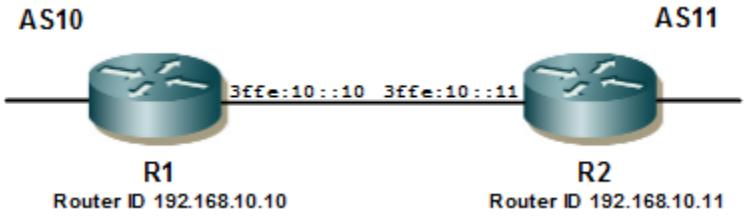


Figure 2-101: Route-Map

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#ipv6 prefix-list myPrefixList seq 5 deny 3ffe:12::/32 ge 48 le 64`	Create an entry in the prefix-list. `myPrefixList` is the name of the map that is created. `5` and `10` specify the sequence number or position of this specific route map. `deny` specifies the packets are to be rejected. `permit` specifies the packets are to be allowed. `48` and `64` are the minimum and maximum prefix lengths, respectively, to be matched.
`(config)#ipv6 prefix-list myPrefixList seq 10 permit any`	Create another entry in the `myPrefixList` map. `10` specifies the sequence number or position of this specific route map. `permit any` specifies accept all packets of any length.
`(config)#route-map myPrefixList permit 1`	Enter Route-map mode.
`(config-route-map)#match ipv6 address prefix-list myPrefixList`	Set the match criteria. In this case, if the route-map name matches `myPrefixList`, the packets from the first sequence will be denied.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 10`	Define the routing process. The number `10` specifies the AS number of R1.
`(config-router)#bgp router-id 192.168.10.10`	Configure a fixed Router ID (`192.168.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10:11 remote-as 11`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::11`) and the AS number (`11`) of neighbor R2.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.

`#configure terminal`	Enter Configure mode.
`(config)#ipv6 prefix-list myPrefixList seq 5 deny 3ffe:12::/32 ge 48 le 64`	Create an entry in the prefix-list. `myPrefixList` is the name of the map that is created. `5` and `10` specify the sequence number or position of this specific route map. `deny` specifies the packets are to be rejected. `permit` specifies the packets are to be allowed. `48` and `64` are the minimum and maximum prefix lengths, respectively, to be matched.
`(config)#ipv6 prefix-list myPrefixList seq 10 permit any`	Create another entry in the `myPrefixList` map. `10` specifies the sequence number or position of this specific route map. `permit any` specifies accept all packets of any length.
`(config)#route-map myPrefixList permit 1`	Enter Route-map mode.
`(config-route-map)#match ipv6 address prefix-list myPrefixList`	Set the match criteria. In this case, if the route-map name matches `myPrefixList`, the packets from the first sequence will be denied.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config-router-af)#neighbor 3ffe:10::11 activate`	Activate the neighbor `R2(3ffe:10::11)`, and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:10::11 route-map myPrefixList in`	Apply the route-map `myPrefixList` to all incoming routes.
`(config-router-af)#exit-address-family`	Exit Address Family mode, and return to Router mode.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

R2

`(config)#router bgp 11`	Define the routing process. The number `11` specifies the AS number of `R2`.
`(config-router)#bgp router-id 192.168.10.11`	Configure a fixed Router ID (`192.168.10.11`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::10 remote-as 10`	Define the BGP neighbor (R1), and establish a TCP session by specifying the IPv6 address (`3ffe:10::10`) and the AS number (`10`) of neighbor `R1`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#network 3ffe:11::/48`	Announce the IPv6 network prefix (`3ffe:11::/48`).
`(config-router-af)#network 3ffe:12::/48`	Announce the IPv6 network prefix (`3ffe:12::/48`).
`(config-router-af)#neighbor 3ffe:10::10 activate`	Activate the neighbor `R1(3ffe:10::10)`, and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#exit-address-family`	Exit Address Family mode, and return to `Router` mode.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors, show bgp ipv6, show bgp ipv6 prefix-list

Route Reflector

Use Route Reflectors to reduce the iBGP mesh inside an AS. In this example, R2, R5, and R4 would have to maintain a full mesh among themselves, but by making R5 the Route Reflector, R2 (Client1) has an iBGP session with RR only, and not with R4 (Client 2). The routes learned from R2 are advertised to the other clients, and to iBGP peers outside the cluster; the iBGP routes learned from iBGP peers outside the cluster are advertised to the R2. This reduces the iBGP peer connections in AS1.

Topology

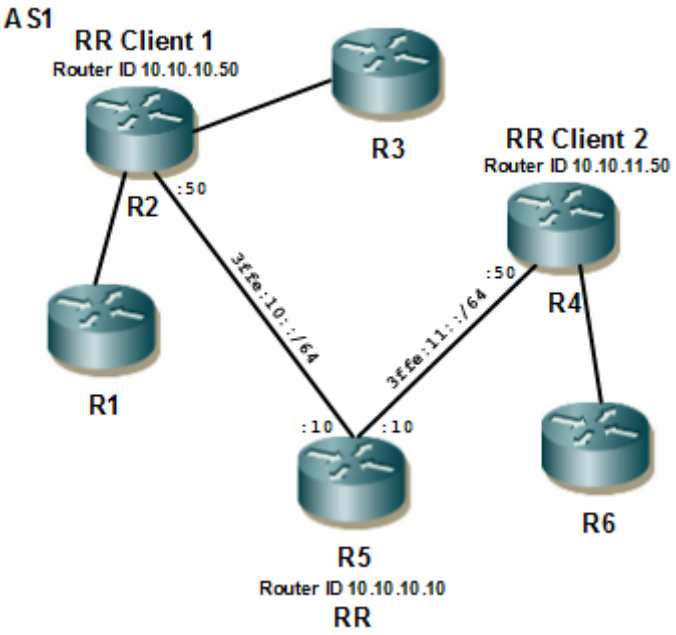


Figure 2-102: BGP4+ Route Reflector

Configuration

RR (R5)

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 1`	Define the routing process. The number 1 specifies the AS number of R5 (RR).
`(config-router)#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::50 remote-as 1`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::50`) and the AS number (`1`) of neighbor R2.

`(config-router)#neighbor 3ffe:11::50 remote-as 1`	Define the BGP neighbor (R4), and establish a TCP session by specifying the IPv6 address (`3ffe:11::50`)and the AS number(`1`) of neighbor R4.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::50 activate`	Activate the neighbor R2(`3ffe:10::50`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:10::50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R2 as its client.
`(config-router-af)#neighbor 3ffe:11::50 activate`	Activate the neighbor R4(`3ffe:11::50`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:11::50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R4 as its client.

RR Client 1 (R2)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of R2 (RR Client 1).
`(config-router)#bgp router-id 10.10.10.50`	Configure a fixed Router ID (`10.10.10.50`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::10 remote-as 1`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:10::10`) and the AS number(`1`) of neighbor R5.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::10 activate`	Activate the neighbor (`3ffe:10::10`), and enable exchange of IPv6 address prefix types with this neighbor.

RR Client 2 (R4)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of R4 (RR Client 2).
`(config-router)#bgp router-id 10.10.11.50`	Configure a fixed Router ID (`10.10.11.50`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:11::10 remote-as 1`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:11::10`) and the AS number(`1`) of the neighbor.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:11::10 activate`	Activate the neighbor (`3ffe:11::10`), and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Confederations

In this example, AS1 contains three Confederated Autonomous Systems--AS 1000, AS 1001 and AS 1002. To any outside AS, the overall Confederation is a single AS, AS1. Confederation eBGP is run between R2 and R5, and between R5 and R7. R2 is configured so that its local AS is 1000. Its peer connection to R5 is set up like any other eBGP session. The `bgp confederation identifier` command informs the router that it is a member of a Confederation and passes the Confederation ID. The `bgp confederation peers` command lists the member AS to which R2 is connected. The same command tells the BGP process that the eBGP connection is a Confederation eBGP, rather than a normal eBGP.

Topology

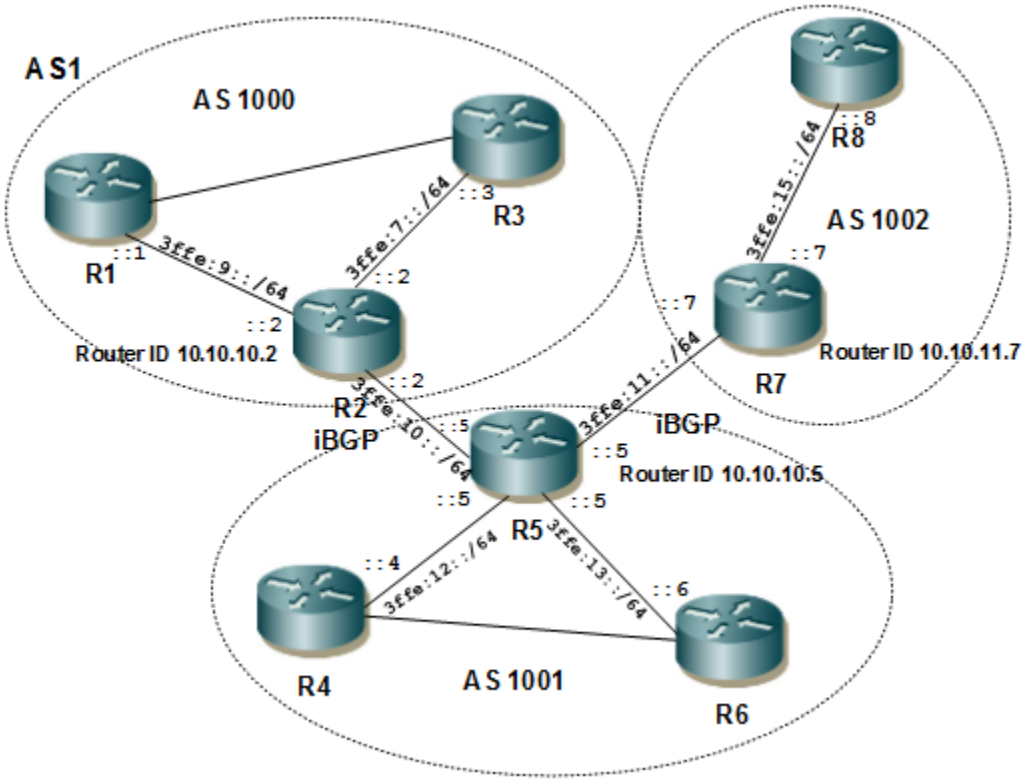


Figure 2-103: BGP4+ Confederations

Configuration

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 1000`	Define the routing process. The number `1000` specifies the AS number of R2.
`(config-router)#bgp router-id 10.10.10.2`	Configure a fixed Router ID (`10.10.10.2`) for the BGP4+ routing process.

`(config-router)#bgp confederation identifier 1`	Specify the BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
`(config-router)#bgp confederation peers 1001 1002`	Specify ASs `1001` and `1002` as confederation peers, making them members of the Confederation.
`(config-router)#neighbor 3ffe:10::5 remote-as 1001`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:10::5`) and the AS number (`1001`) of neighbor R5.
`(config-router)#neighbor 3ffe:9::1 remote-as 1000`	Define the BGP neighbor (R1), and establish a TCP session by specifying the IPv6 address (`3ffe:9::1`) and the AS number (`1000`) of neighbor R1.
`(config-router)#neighbor 3ffe:7::3 remote-as 1000`	Define the BGP neighbor (R3), and establish a TCP session by specifying the IPv6 address (`3ffe:7::3`) and the AS number (`1000`) of neighbor R3.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::5 activate`	Activate neighbor R5 (`3ffe:10::5`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:9::1 activate`	Activate neighbor R1 (`3ffe:9::1`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:7::3 activate`	Activate neighbor R3 (`3ffe:7::3`), and enable exchange of IPv6 address prefix types with this neighbor.

R5

`(config)#router bgp 1001`	Define the routing process. The number `1001` specifies the AS number of R5.
`(config-router)#bgp router-id 10.10.10.5`	Configure a fixed Router ID (`10.10.10.5`) for the BGP4+ routing process.
`(config-router)#bgp confederation identifier 1`	Specify the BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
`(config-router)#bgp confederation peers 1000 1002`	Specify ASs `1001` and `1002` as confederation peers, making them members of the Confederation.
`(config-router)#neighbor 3ffe:10::2 remote-as 1000`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::2`) and the AS number (`1000`) of neighbor R2.
`(config-router)#neighbor 3ffe:11::7 remote-as 1002`	Define the BGP neighbor (R7), and establish a TCP session by specifying the IPv6 address (`3ffe:11::7`) and the AS number (`1002`) of neighbor R7.
`(config-router)#neighbor 3ffe:12::4 remote-as 1001`	Define the BGP neighbor (R4), and establish a TCP session by specifying the IPv6 address (`3ffe:12::4`) and the AS number (`1001`) of neighbor R4.
`(config-router)#neighbor 3ffe:13::6 remote-as 1001`	Define the BGP neighbor (R6), and establish a TCP session by specifying the IPv6 address (`3ffe:13::6`) and the AS number (`1001`) of neighbor R6.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.

`(config-router-af)#neighbor 3ffe:10::2 activate`	Activate the neighbor R2(`3ffe:10::2`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:11::7 activate`	Activate the neighbor R7(`3ffe:11::7`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:12::4 activate`	Activate the neighbor R4(`3ffe:12::4`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:13::6 activate`	Activate the neighbor R6(`3ffe:13::6`), and enable exchange of IPv6 address prefix types with this neighbor.

R7

`(config)#router bgp 1002`	Define the routing process. The number `1002` specifies the AS number of R7.
`(config-router)#bgp router-id 10.10.11.7`	Configure a fixed Router ID (`10.10.11.7`) for the BGP4+ routing process.
`(config-router)#bgp confederation identifier 1`	Specify BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
`(config-router)#bgp confederation peers 1000 1001`	Specify ASs `1000` and `1001` as confederation peers, making them members of the Confederation.
`(config-router)#neighbor 3ffe:11::5 remote-as 1001`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:11::5`)and the AS number(`1001`)of neighbor R5.
`(config-router)#neighbor 3ffe:15::8 remote-as 1002`	Define the BGP neighbor (R8), and establish a TCP session by specifying the IPv6 address (`3ffe:15::8`)and the AS number(`1002`)of neighbor R8.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:11::5 activate`	Activate the neighbor R5(`3ffe:11::5`), and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:15::8 activate`	Activate the neighbor R8(`3ffe:15::8`), and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

BGP4+ Graceful Restart

Using BGP+ graceful restart, the data-forwarding plane of a router can continue to process and forward packets, even if the control plane (which is responsible for determining best paths) fails.

Topology

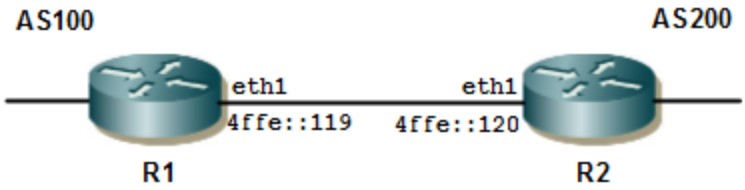


Figure 2-104: BGP4+ Graceful Restart

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#bgp graceful-restart`	Enable BGP graceful restart support.
`(config-router)#neighbor 4ffe::120 remote-as 200`	Specify the neighbor's IP address (`4ffe::120`) and the ASN value of the neighbor (`200`).
`(config-router)#address-family ipv6 unicast`	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
`(config-router-af)#neighbor 4ffe::120 activate`	Specify the neighbor's IPv6 address (`4ffe::120`), and activate the neighbor.
`(config-router-af)#neighbor 4ffe::120 capability graceful-restart`	Specify the neighbor's IPv6 address (`4ffe::120`) for which the graceful restart capability is supported.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#bgp graceful-restart`	Enable BGP graceful restart support.
`(config-router)#bgp graceful-restart restart-time 120`	Configure the maximum time (`120`) required for neighbor(s) to restart.
`(config-router)#bgp graceful-restart stalepath-time 120`	Configure the maximum time (`120`) to retain stale paths from the restarting neighbor(s).
`(config-router)#neighbor 4ffe::119 remote-as 100`	Specify the neighbor's IP address (`4ffe::119`) and the ASN value of the neighbor (`100`).
`(config-router)#address-family ipv6 unicast`	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
`(config-router-af)#neighbor 4ffe::119 activate`	Specify the neighbor's IPv6 address (`4ffe::119`), and activate the neighbor.
`(config-router-af)#neighbor 4ffe::119 capability graceful-restart`	Specify the neighbor's IPv6 address (`4ffe::119`) for which the graceful restart capability is supported.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show bgp ipv6, show ipv6 route database bgp, show ipv6 route database, show ipv6 route

Configure BGP4+ Distance

Administrative distance in BGP+ can be configured for a specific address family.

This example shows configuring the BGP administrative distance for the IPv6 address family.

Topology

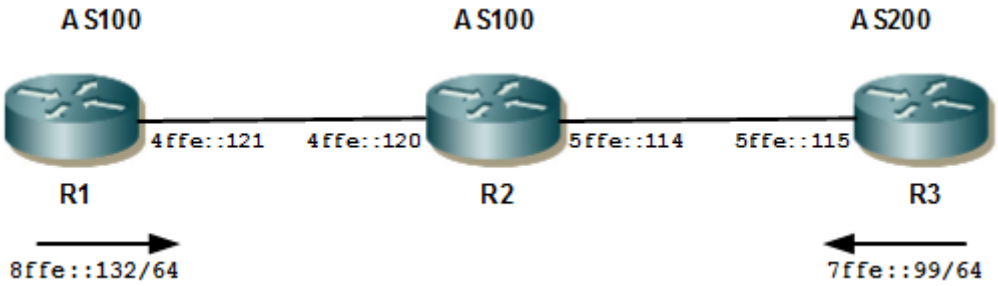


Figure 2-105: BGP4+ Distance

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#network 8ffe::132/64`	Specify the network to be advertised by the BGP routing process.
`(config-router)#neighbor 4ffe::120 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Address-Family mode.
`(config-router-af)#neighbor 4ffe::120 activate`	Activate the IPv6 neighbor.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 4ffe::121 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#neighbor 5ffe::115 remote-as 200`	Specify the neighbor's IP address and the ASN value of another neighbor.

`(config-router)#address-family ipv6 unicast`	Enter IPv6 Address-Family mode.
`(config-router-af)#aggregate-address 2ffe::102/64 summary-only`	Configure an IPv6 non-AS-set aggregate route on R2. The local distance will be applied to this route.
`(config-router-af)#neighbor 4ffe::121 activate`	Activate the IPv6 neighbor.
`(config-router-af)#neighbor 5ffe::115 activate`	Activate the IPv6 neighbor.
`(config-router-af)#distance 12 13 11`	Configure the administrative distance for external, internal, and local routes received in IPv6 Address-Family mode.

R3

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#network 7ffe::99/64`	Specify the network to be advertised by the BGP routing process.
`(config-router)#neighbor 5ffe::114 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Address-Family mode.
`(config-router-af)#neighbor 5ffe::114 activate`	Activate the IPv6 neighbor.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show ipv6 route database bgp, show ipv6 route database, show ipv6 route, show bgp ipv6

BGP4+ Graceful Reset

The graceful restart mechanism for BGP+ session reset (the BGP+ daemon is not restarted) is used so that any changes in network configuration do not affect packet forwarding. The `bgp graceful-restart graceful-reset` CLI invokes graceful restart when a configuration change forces a peer reset. Graceful restart is invoked only when these CLI configuration changes force a peer reset.

Topology

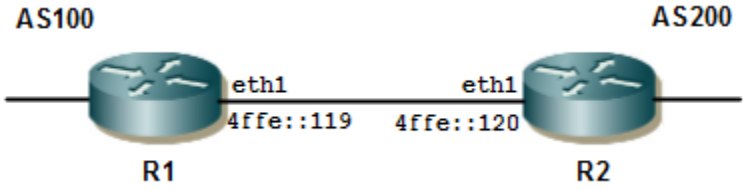


Figure 2-106: BGP4+ Graceful Reset

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#bgp graceful-restart`	Enable BGP graceful restart support.
`(config-router)#bgp graceful-restart graceful-reset`	Configure to invoke graceful restart when a configuration change forces a peer reset.
`(config-router)#neighbor 4ffe::120 remote-as 200`	Specify the neighbor's IP address (`4ffe::120`) and the ASN value of the neighbor (`200`).
`(config-router)#address-family ipv6 unicast`	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
`(config-router-af)#neighbor 4ffe::120 activate`	Specify the neighbor's IPv6 address(`4ffe::120`), and activate the neighbor.
`(config-router-af)#neighbor 4ffe::120 capability graceful-restart`	Specify the neighbor's IPv6 address (`4ffe::120`) for which the graceful restart capability is supported.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#bgp graceful-restart`	Enable BGP graceful restart support.
`(config-router)#bgp graceful-restart graceful-reset`	Configure to invoke graceful restart when a configuration change forces a peer reset.
`(config-router)#neighbor 4ffe::119 remote-as 100`	Specify the neighbor's IP address (`4ffe::119`) and the ASN value of the neighbor (`100`).
`(config-router)#address-family ipv6 unicast`	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
`(config-router-af)#neighbor 4ffe::119 activate`	Specify the neighbor's IPv6 address(`4ffe::119`), and activate the neighbor.
`(config-router-af)#neighbor 4ffe::119 capability graceful-restart`	Specify the neighbor's IPv6 address (`4ffe::119`) for which the graceful restart capability is supported.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show bgp ipv6, show ipv6 route database bgp, show ipv6 route database, show ipv6 route

CHAPTER 3 BGP Graceful Restart Configuration

During a BGP restart, all BGP peers detect that a session had gone down and come back up. OcNOS invalidates the associated portion of the IP forwarding cache, does a BGP route re-computation, and generates BGP routing updates. The forwarding tables become corrupted and unstable.

Graceful restart helps minimize these negative effects on routing caused by a BGP restart by allowing the restarting BGP router to temporarily retain routing information and continue forwarding packets while BGP restarts. In this way, even while a router rebuilds routing and forwarding tables, the router continues to operate across the TCP connection.

Graceful restart allows a restarting router, and its neighbors, to continue forwarding packets, without disrupting network performance. Because neighboring routers assist in the restart, the restarting router can quickly resume full operation.

The graceful restart capability extends to the case when a configuration change forces a peer reset.

Graceful reset is a refinement of graceful restart to help ensure smooth restarts when a configuration change forces BGP peer reset.

In addition, graceful restart is available for BGP with MPLS, when BGP is used to distribute MPLS-VPN labels. Without the graceful restart capability, when BGP distributes MPLS-VPN labels, a BGP route withdrawal accompanies the associated label withdrawal. This causes a routing flap and a BGP route re-computation, generating BGP routing updates, and unnecessary disruption in the forwarding tables. Also, when BGP goes down, label-switched routers (LSRs) clear FEC label bindings (for VPN routes) learned from the restarting LSR. As a result, MPLS forwarding is impacted across the restart.

The graceful restart and graceful reset capabilities provide a way to save MPLS forwarding states in NSM. These capabilities also synchronize with the VRF table when BGP goes down in the control plane. This feature is supported for the VPNv4 address family.

Topology

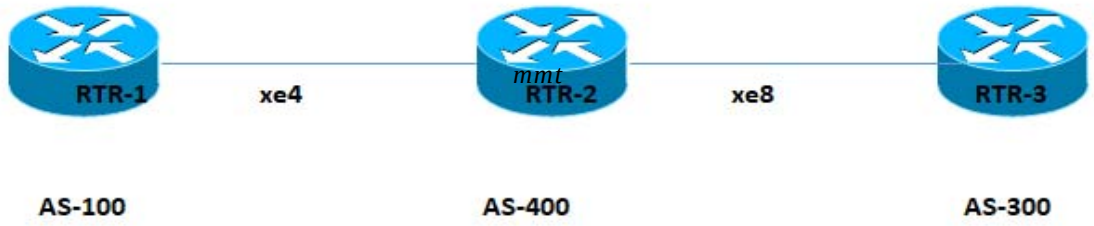


Figure 3: Device topology for BGP in VR/VRF

RTR1

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 1.1.1.11.1.1.1/32 secondary`	Configure ip address on loopback.

(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode for eth2.
(config-if)#ip address 10.10.10.1/24	Configure ip address on eth2.
(config-if)#exit	Exit interface mode for eth2.
(config)# router bgp 100	Enter router bgp mode.
(config-router)# bgp router-id 1.1.1.11.1.1.1	Configure bgp router-id same as loopback ip address.
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP.
(config-router)#redistribute connected	Redistributing connected Routes inside BGP.
(config-router)# neighbor 10.10.10.2 remote-as 400	Configure Neighbor for AS-400.
(config-router)# neighbor 10.10.10.2 capability graceful-restart	Configure GR capability inside router bgp.
(config-router)#end	Exit router BGP mode.

RTR2

#configure terminal	Enter Configuration mode.
(config)#interface lo	Enter interface mode for loopback.
(config-if)#ip address 2.2.2.22.2.2.2/32 second-ary	Configure ip address on loopback.
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode for eth1.
(config-if)#ip address 10.10.10.2/24	Configure ip address on eth1.
(config-if)#exit	Exit interface mode for eth1.
(config)#interface xe8	Enter interface mode for eth2.
(config-if)#ip address 20.20.20.1/24	Configure ip address on eth2.
(config-if)#exit	Exit interface mode for eth2.
(config)#router bgp 400	Enter router BGP mode.
(config-router)# bgp router-id 2.2.2.22.2.2.2	Configure bgp router-id same as loopback ip address.
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP.
(config-router)#redistribute connected	Redistributing connected Routes inside BGP.
(config-router)# neighbor 10.10.10.1 remote-as 100	Configure Neighbor for AS-100.
(config-router)# neighbor 10.10.10.1 capability graceful-restart	Configure GR capability inside router bgp.
(config-router)# neighbor 20.20.20.2 remote-as 300	Configure Neighbor for AS-300.
(config-router)# neighbor 20.20.20.2 capability graceful-restart	Configure GR capability inside router bgp
(config-router)#end	Exit router ospf mode.

RTR3

#configure terminal	Enter Configuration mode.
(config)#interface lo	Enter interface mode for loopback.
(config-if)#ip address 3.3.3.33.3.3.3/32 secondary	Configure ip address on loopback.
(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter interface mode for eth2.
(config-if)#ip address 20.20.20.2/24	Configure ip address on eth2.
(config-if)#exit	Exit interface mode for eth2.
(config)# router bgp 300	Enter router BGP mode.
(config-router)# bgp router-id 3.3.3.33.3.3.3	Configure bgp router-id same as loopback ip address.
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP.
(config-router)#redistribute connected	Redistributing connected Routes inside BGP.
(config-router)# neighbor 20.20.20.1 remote-as 400	Configure Neighbor for AS-400.
(config-router)# neighbor 20.20.20.1 capability graceful-restart	Configure GR capability inside router bgp.
(config-router)#end	Exit router BGP mode.

Validation

RTR1

```
RTR1#show  bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 400, local AS 100, external link
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:03:31
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 13 messages, 1 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  3 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
 Graceful-restart Status:
  Remote restart-time is 90 sec
```

```
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 60024
Nexthop: 10.10.10.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:03:36, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show ip route databaseCodes: K - kernel, C - connected, S - static, R - RIP,
B - BGP O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C*>1.1.1.11.1.1.1/32 is directly connected, lo, 00:10:23
B*>2.2.2.22.2.2.2/32 [20/0] via 10.10.10.2, xe4, 00:03:56
B*>3.3.3.33.3.3.3/32 [20/0] via 10.10.10.2, xe4, 00:00:56
C*>10.10.10.0/24 is directly connected, xe4, 00:09:37
B*>20.20.20.0/24 [20/0] via 10.10.10.2, xe4, 00:03:56
C*>127.0.0.0/8 is directly connected, lo, 00:28:58

Gateway of last resort is not set
```

RTR2

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*>1.1.1.11.1.1.1/32 [20/0] via 10.10.10.1, xe4, 00:03:52
C*>2.2.2.22.2.2.2/32 is directly connected, lo, 00:07:36
B*>3.3.3.33.3.3.3/32 [20/0] via 20.20.20.2, xe8, 00:00:57

C*>10.10.10.0/24 is directly connected, xe4, 00:07:12 C*>20.20.20.0/24 is
directly connected, xe8, 00:06:31
C*>127.0.0.0/8 is directly connected, lo, 00:25:32

Gateway of last resort is not set

RTR2#show bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 400, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:04:28
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 43 messages, 1 notifications, 0 in queue
  Sent 41 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  3 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 10.10.10.2, Local port: 60050
Foreign host: 10.10.10.1, Foreign port: 179
Nexthop: 10.10.10.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:33, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 20.20.20.2, remote AS 300, local AS 400, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:04:22
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 31 messages, 2 notifications, 0 in queue
  Sent 40 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  4 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 20.20.20.1, Local port: 179
Foreign host: 20.20.20.2, Foreign port: 56342
Nexthop: 20.20.20.1
Nexthop global: ::
Nexthop local: ::
```

```
BGP connection: non shared network
Last Reset: 00:04:22, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

RTR2#
```

RTR3

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*> 1.1.1.11.1.1.1/32 [20/0] via 20.20.20.1, xe8, 00:01:15
B*> 2.2.2.22.2.2.2/32 [20/0] via 20.20.20.1, xe8, 00:01:15
C*> 3.3.3.3/32 is directly connected, lo
B*> 10.10.10.0/24 [20/0] via 20.20.20.1, xe8, 00:01:15
C*> 20.20.20.0/24 is directly connected, xe8
C*> 127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
RTR3#show bgp neighbors
BGP neighbor is 20.20.20.1, remote AS 400, local AS 300, external link
  BGP version 4, local router ID 3.3.3.3, remote router ID 2.2.2.2
  BGP state = Established, up for 00:06:47
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 1 notifications, 0 in queue
  Sent 38 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  4 accepted prefixes
  0 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 20.20.20.2, Local port: 56342
Foreign host: 20.20.20.1, Foreign port: 179
Nexthop: 20.20.20.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

```
Last Reset: 00:06:52, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

RTR3#
```

Validation After BGP Graceful Restart

RTR2

```
#write
Building configuration... [OK]

#restart bgp graceful
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[10.10.10.1] Session down as GR configured/unconfigured
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[10.10.10.1] Session down due to config deletion
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[20.20.20.2] Session down as GR configured/unconfigured
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[20.20.20.2] Session down due to config deletion

#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked

> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*>p 1.1.1.1/32 [20/0] via 10.10.10.1, xe4, 00:19:31
C*>2.2.2.2/32 is directly connected, lo, 00:50:45
B*>p 3.3.3.3/32 [20/0] via 20.20.20.2, xe8, 00:19:32
C*>10.10.10.0/24 is directly connected, xe4, 00:50:21 C*>20.20.20.0/24 is
directly connected, xe8, 00:49:40
C*>127.0.0.0/8 is directly connected, lo, 01:08:41 Gateway of last resort is
not set
#show rib forwarding-timer
Protocol-Name GR-State Time Remaining (sec)Disconnected-time BGPACTIVE572001/
06/07 19:50:38
```

RTR1

```
#show ip bgp
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - Labeled, S Stale
Origin codes: i - IGP, e - EGP,? - incomplete
```

```
NetworkNext HopMetricLocPrfWeightPath
*>1.1.1.1/32
0.0.0.0010032768?
S>2.2.2.2/32
10.10.10.201000400?
S>3.3.3.3/32
10.10.10.201000400300?
*>10.10.10.0/240.0.0.0010032768?
S10.10.10.201000400?
S>20.20.20.0/2410.10.10.201000400?

Total number of prefixes 5
```

RTR3

```
#sh ip bgp
BGP table version is 14, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

NetworkNext HopMetricLocPrfWeightPath
S>1.1.1.1/32
20.20.20.101000400 100?
S>2.2.2.2/32
20.20.20.101000400 ?
*>3.3.3.3/32
0.0.0.0010032768?
S>10.10.10.0/2420.20.20.101000400 ?
*>20.20.20.0/240.0.0.0010032768?
S20.20.20.101000400 ?

Total number of prefixes 5
```

CHAPTER 4 OSPFv2

This chapter contains basic OSPFv2 (Open Shortest Path First) configuration examples.

Enable OSPF on an Interface

The diagram shows the minimum configuration required to enable OSPF on an interface. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

Topology

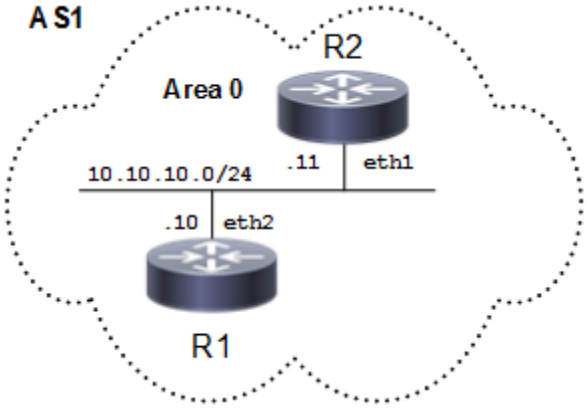


Figure 4-1: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID (`200`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

Validation

R1

```
#show ip ospf
 Routing Process "ospf 100" with ID 10.12.26.88
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:08.102 ago
        SPF algorithm executed 3 times
        Number of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 13 sent 19, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
No authentication
```

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/Backup     00:00:39    10.10.10.11     eth2
0


#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R2

```
#show  ip ospf
 Routing Process "ospf 200" with ID 10.12.26.89
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 5
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:45.638 ago
        SPF algorithm executed 4 times
        Number of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface
eth1 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
```

```
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 31, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
No authentication


#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 200 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
10.12.26.88      1   Full/DR        00:00:33   10.10.10.10    eth1
0

#show ip ospf route

OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

Set Priority

This example shows how to set the priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured to have a priority of 10, which is higher than the default priority (1) of R1 and R2; making it the DR.

Topology

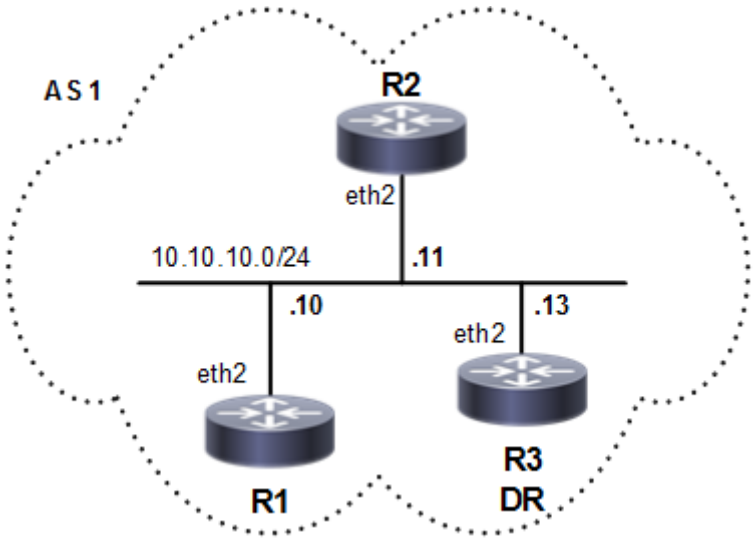


Figure 4-2: Set OSPF Priority

R3

`#configure terminal`	Enter configure mode
`(config)``#interface eth2`	Enter interface mode.
`(config-if)``#ip ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).
`(config-if)``#exit`	Exit interface mode.
`(config)``#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)``#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID (`200`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

Validation

R1

```
#sh ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/DROther    00:00:39    10.10.10.11     eth2
0
10.12.26.90      10   Full/DR         00:00:32    10.10.10.13     eth2
0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 19, DD received 6 sent 8
  LS-Req received 2 sent 2, LS-Upd received 16 sent 6
  LS-Ack received 8 sent 7, Discarded 0
  No authentication

#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
```

```
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end
```

R2

```
#show running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
```

```
!
interface eth1
!
interface eth2
 ip address 10.10.10.11/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 200
 network 10.10.10.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end

#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 200 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88     1   Full/Backup     00:00:30   10.10.10.10    eth2
0
10.12.26.90    10   Full/DR        00:00:31   10.10.10.13    eth2
0
R2#

R2#show ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 71 sent 36, DD received 7 sent 7
  LS-Req received 2 sent 2, LS-Upd received 9 sent 4
  LS-Ack received 3 sent 4, Discarded 1
  No authentication
```

R3

```
#show running-config
!
```

```
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp
data-center-bridging enable
ethernet cfm enable
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.90/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.13/24
 ip ospf priority 10
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end

#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:33    10.10.10.10     eth2
0
10.12.26.89       1   Full/DROther    00:00:30    10.10.10.11     eth2
0
```

```
#show ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.13/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 10, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 99 sent 60, DD received 8 sent 6
  LS-Req received 2 sent 2, LS-Upd received 9 sent 12
  LS-Ack received 9 sent 6, Discarded 1
```

No authentication

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, Interface eth0 is in Area 0, and Interface eth1 is in Area 1.

Topology

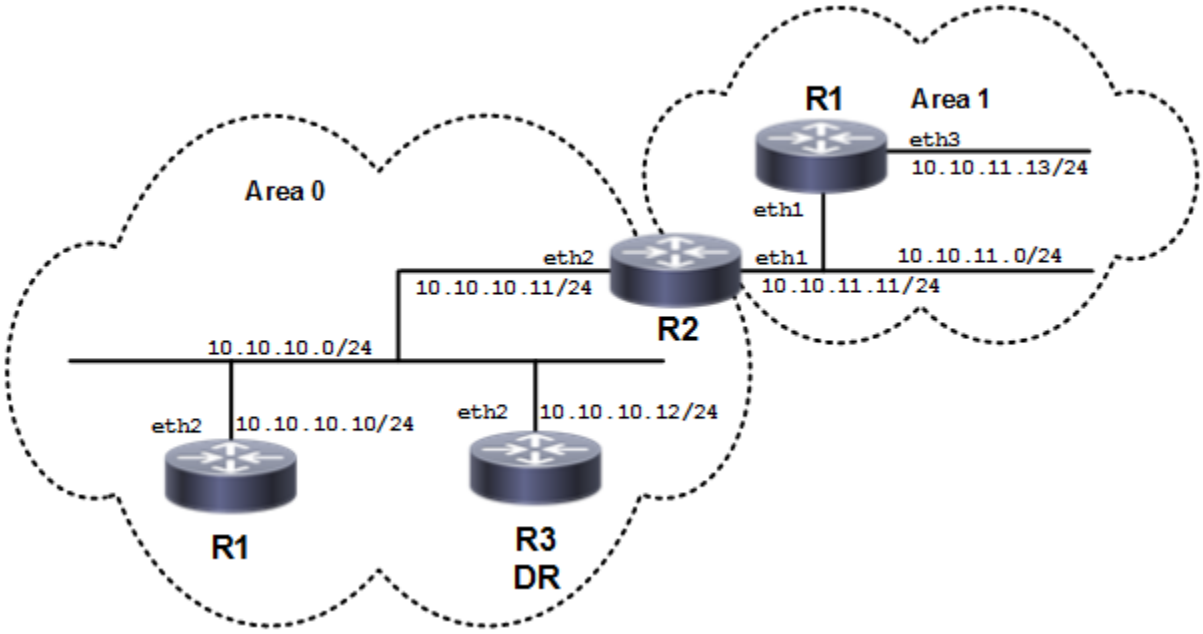


Figure 4-3: OSPF ABR Topology

Configuration

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.
`(config-router)#network 10.10.11.0/24 area 1`	Define the other interface `(10.10.11.0/24)` on which OSPF runs, and associate the area ID `(1)` with the interface.

Validation

R2

```
#show running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 10.10.11.11/24
!
interface eth2
 ip address 10.10.10.11/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
```

```
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.1

!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip ospf
 Routing Process "ospf 100" with ID 10.12.26.89
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 9
 Number of LSA received 18
 Number of areas attached to this router: 2
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:01:54.085 ago
        SPF algorithm executed 7 times
        Number of LSA 11. Checksum 0x0428ac
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:41.737 ago
SPF algorithm executed 3 times
        Number of LSA 8. Checksum 0x043ce4
 Dste Staus: Disabled

#show ip ospf interface
eth2 is up, line protocol is up
```

```
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 66 sent 38, DD received 11 sent 7
  LS-Req received 2 sent 2, LS-Upd received 15 sent 14
  LS-Ack received 14 sent 10, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.1, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.13
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 22 sent 24, DD received 3 sent 9
  LS-Req received 1 sent 1, LS-Upd received 4 sent 5
  LS-Ack received 4 sent 3, Discarded 0
  No authentication

#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 100 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88      1   Full/Backup     00:00:34   10.10.10.10    eth2
0
10.12.26.90      1   Full/DROther    00:00:32   10.10.10.12    eth2
0
10.12.26.92      1   Full/DR        00:00:33   10.10.11.13    eth1
0

#show ip ospf database

            OSPF Router with ID (10.12.26.89) (Process ID 100 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
10.12.26.88     10.12.26.88      365     0x80000005 0x10bc 1
10.12.26.89     10.12.26.89      312     0x80000006 0x0fb8 1
10.12.26.90     10.12.26.90      363     0x80000003 0x10b8 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.11     10.12.26.89      364     0x80000002 0xe7fd
```

```
                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum     Route
10.10.11.0      10.12.26.89      312     0x80000001 0x95fd 10.10.11.0/24

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         10.12.26.88      363     0x80000003 0xa972 1
1.0.0.1         10.12.26.89      362     0x80000003 0xad6c 1
1.0.0.1         10.12.26.90      363     0x80000001 0xb564 1
1.0.0.10        10.12.26.88      363     0x80000003 0x0a32 10
1.0.0.10        10.12.26.89      362     0x80000002 0x2417 10
1.0.0.10        10.12.26.90      363     0x80000001 0x3efb 10

                Router Link States (Area 0.0.0.1)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
10.12.26.89     10.12.26.89      245     0x80000004 0x3d88 1
10.12.26.92     10.12.26.92      241     0x80000004 0x2698 1

                Net Link States (Area 0.0.0.1)
Link ID         ADV Router       Age     Seq#       CkSum
10.10.11.13     10.12.26.92      246     0x80000001 0x6ffb

                Summary Link States (Area 0.0.0.1)

Link ID         ADV Router       Age     Seq#       CkSum     Route
10.10.10.0      10.12.26.89      312     0x80000001 0xa0f3 10.10.10.0/24

                Area-Local Opaque-LSA (Area 0.0.0.1)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         10.12.26.89      243     0x80000001 0xb16a 1
1.0.0.1         10.12.26.92      244     0x80000001 0xbd58 1
1.0.0.8         10.12.26.89      234     0x80000002 0x96a2 8
1.0.0.8         10.12.26.92      244     0x80000001 0xc272 8
```

Redistribute Routes into OSPF

In this example, the configuration causes BGP routes to be imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

Topology

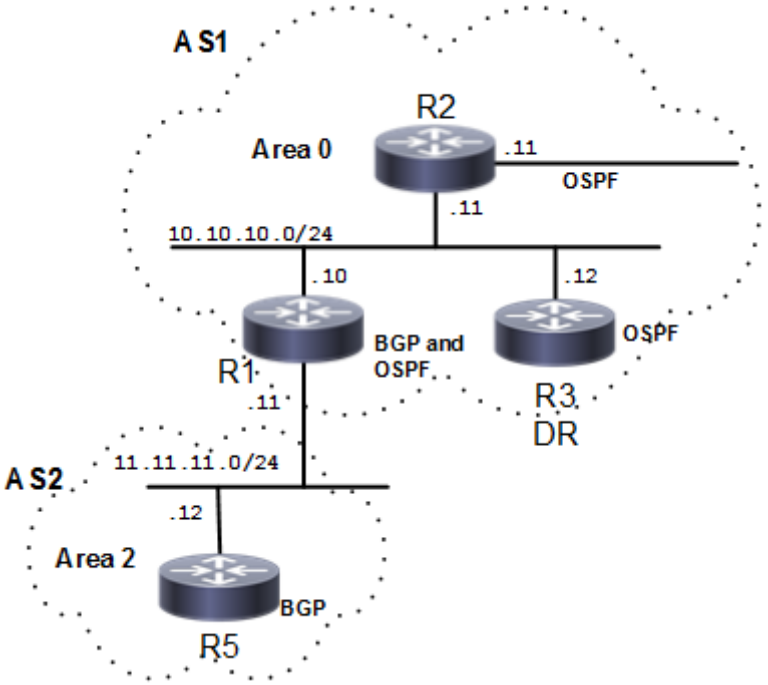


Figure 4-4: Redistribute Routes

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#redistribute bgp`	Specify redistributing routes from other routing protocol (BGP) into OSPF.

Validation

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
```

Cost

A route can be made the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 1. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 1+100 = 101

R3: 1+150 = 151

Therefore, R1 chooses R2 as its next hop to destination 10.10.14.0/24 because it has the lower cost.

Topology

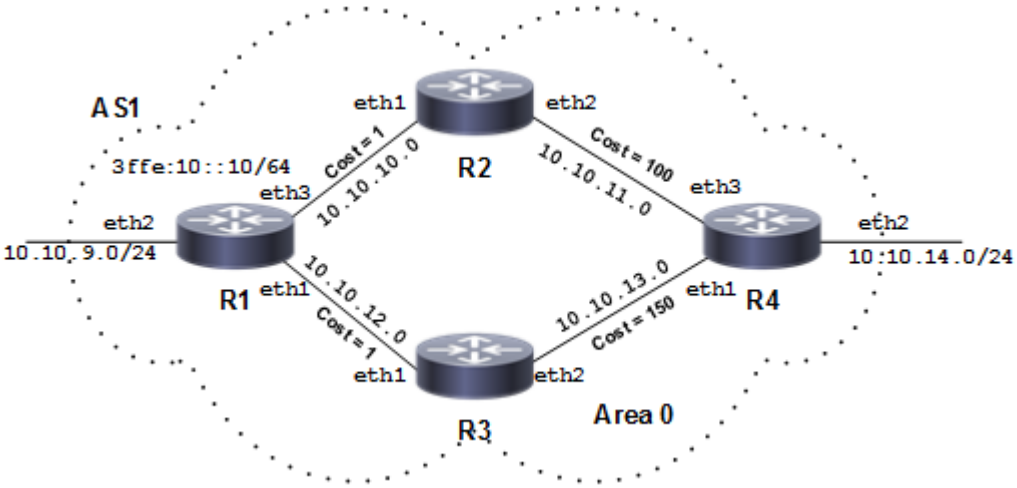


Figure 4-5: Configure Cost Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.9.0/24 area 0`
`(config-router)#network 10.10.10.0/24 area 0`
`(config-router)#network 10.10.12.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID `0` specifies the backbone area).

R2

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf cost 100`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R3

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf cost 150`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.12.0/24 area 0` `(config-router)#network 10.10.13.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R4

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.11.0/24 area 0`
`(config-router)#network 10.10.13.0/24 area 0`
`(config-router)#network 10.10.14.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0

#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
```

```
    Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
    Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:03
    Neighbor Count is 1, Adjacent neighbor count is 1
    Suppress hello for 0 neighbor(s)
    Hello received 43 sent 69, DD received 3 sent 4
    LS-Req received 1 sent 1, LS-Upd received 16 sent 18
    LS-Ack received 10 sent 11, Discarded 0
    No authentication
  eth2 is up, line protocol is up
    Internet Address 10.10.9.10/24, Area 0.0.0.0, MTU 1500
    Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
  BROADCAST, Cost: 1
    Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
    Designated Router (ID) 10.12.26.88, Interface Address 10.10.9.10
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)
    Hello received 0 sent 68, DD received 0 sent 0
    LS-Req received 0 sent 0, LS-Upd received 0 sent 0
    LS-Ack received 0 sent 0, Discarded 0
    No authentication
  eth1 is up, line protocol is up
    Internet Address 10.10.12.10/24, Area 0.0.0.0, MTU 1500
    Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
  BROADCAST, Cost: 1
    Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
    Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10
    Backup Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:01
    Neighbor Count is 1, Adjacent neighbor count is 1
    Suppress hello for 0 neighbor(s)
  Hello received 29 sent 66, DD received 3 sent 4
    LS-Req received 1 sent 1, LS-Upd received 10 sent 12
    LS-Ack received 10 sent 9, Discarded 0
    No authentication
```

R2

```
  #sh ip ospf route

  OSPF process 100:
  Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2

  O  10.10.9.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
  C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
  C  10.10.11.0/24 [100] is directly connected, eth2, Area 0.0.0.0
  O  10.10.12.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
  O  10.10.13.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0
  O  10.10.14.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0

  #sh ip ospf interface
```

```
eth2 is up, line protocol is up
  Internet Address 10.10.11.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 100
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 100
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 56 sent 77, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 11 sent 7
  LS-Ack received 4 sent 8, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 74 sent 75, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 18 sent 16
  LS-Ack received 10 sent 12, Discarded 0
  No authentication
```

R3

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.10.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.11.0/24 [102] via 10.10.12.10, eth1, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.14.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.13.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 150
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 150
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
```

```
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 85 sent 94, DD received 3 sent 4
  LS-Req received 0 sent 0, LS-Upd received 3 sent 4
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.12.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10
  Backup Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 92 sent 92, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 12 sent 10
  LS-Ack received 8 sent 10, Discarded 0
  No authentication
```

R4

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [3] via 10.10.11.10, eth3, Area 0.0.0.0
                    via 10.10.13.10, eth1, Area 0.0.0.0
O  10.10.10.0/24 [2] via 10.10.11.10, eth3, Area 0.0.0.0
C  10.10.11.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.12.0/24 [2] via 10.10.13.10, eth1, Area 0.0.0.0
C  10.10.13.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C  10.10.14.0/24 [1] is directly connected, eth2, Area 0.0.0.0

#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 95 sent 96, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 7 sent 11
  LS-Ack received 7 sent 5, Discarded 0
  No authentication
eth2 is up, line protocol is up
  Internet Address 10.10.14.10/24, Area 0.0.0.0, MTU 1500
```

```
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.14.10
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Hello received 0 sent 95, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.13.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
 Hello received 92 sent 93, DD received 4 sent 3
  LS-Req received 0 sent 0, LS-Upd received 4 sent 3
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a non-contiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn, disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

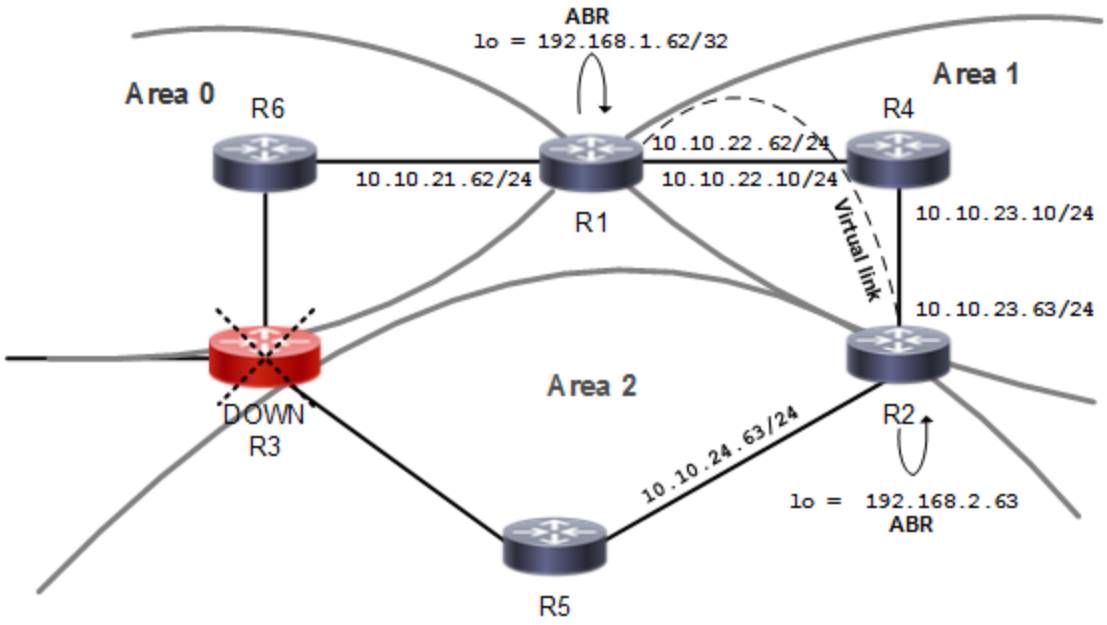


Figure 4-6: Virtual Links Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.1.62/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 192.168.1.62`	Configure the OSPF Router ID (`192.168.1.62`) for this router.
`(config-router)#network 10.10.21.0/24 area 0` `(config-router)#network 10.10.22.0/24 area 1`	Define interfaces on which OSPF runs, and associate the area IDs (`0 and 1`) with the interface.
`(config-router)#area 1 virtual-link 192.168.2.63`	Configure a virtual link between this router R1 and R2 (Router ID `192.168.2.63`) through transit area 1.

R2

`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.2.63/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#ospf router-id 192.168.2.63`	Configure the OSPF Router ID (`192.168.1.63`) for this router.

`(config-router)#network 10.10.23.0/24 area 1`
`(config-router)#network 10.10.24.0/24 area 2`
`(config-router)#network 192.168.2.63/32 area 2`
	Define interfaces on which OSPF runs, and associate the area IDs (`1` and `2`) with the interface.

`(config-router)#area 1 virtual-link 192.168.1.62`	Configure a virtual link between this router R2 and R1 (Router ID `192.168.2.62`) through transit area `1`.

Validation

```
R1#show ip ospf virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
  Transit area 0.0.0.1 via interface eth2
  Hello suppression enabled
  DoNotAge LSA allowed
  Local address 13.13.13.1/32
  Remote address 12.12.12.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  No authentication
    Adjacency state Down

R2#show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface eth1
  Hello suppression enabled
  DoNotAge LSA allowed
  Local address 12.12.12.1/32
  Remote address 13.13.13.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  No authentication
    Adjacency state Init

R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
192.168.20.5     1   Full/DR       00:00:34   13.13.13.2     eth2
0


R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
192.168.20.5     1   Full/DR       00:00:36   12.12.12.2     eth1
0
1.1.1.1           1   Init/ -          00:00:32    13.13.13.1      VLINK0
```

```
R1#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

IA 2.2.2.2/32 [12] via 13.13.13.2, eth2, Area 0.0.0.1
O  12.12.12.0/24 [2] via 13.13.13.2, eth2, Area 0.0.0.1
C  13.13.13.0/24 [1] is directly connected, eth2, Area 0.0.0.1

R2#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.2/32 [10] is directly connected, lo, Area 0.0.0.2
C  12.12.12.0/24 [1] is directly connected, eth1, Area 0.0.0.1
O  13.13.13.0/24 [2] via 12.12.12.2, eth1, Area 0.0.0.1

R1#show ip ospf
 Routing Process "ospf 100" with ID 1.1.1.1
 Process uptime is 39 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 15
 Number of areas attached to this router: 2
MemPool - struct ospf lsa             : (0-16) | Total (16/100000)
blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:10:05.434 ago
        SPF algorithm executed 1 times
```

```
        Number of LSA 3. Checksum 0x01bf9c
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:09:57.432 ago
        SPF algorithm executed 7 times
        Number of LSA 13. Checksum 0x076e78
 Dste Staus: Disabled

R2#show ip ospf
 Routing Process "ospf 100" with ID 2.2.2.2
 Process uptime is 16 hours 48 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 11
 Number of LSA received 12
 Number of areas attached to this router: 3
MemPool - struct ospf lsa             : (0-20) | Total (20/100000)
blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:11:05.618 ago
        SPF algorithm executed 1 times
        Number of LSA 4. Checksum 0x018ce2
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:11:03.619 ago
        SPF algorithm executed 6 times
        Number of LSA 13. Checksum 0x076e78
    Area 0.0.0.2
        Number of interfaces in this area is 1(1)
```

```
        Number of fully adjacent neighbors in this area is 0
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:11:05.618 ago
        SPF algorithm executed 3 times
        Number of LSA 3. Checksum 0x0139cf
Dste Staus: Disabled
```

OSPF Authentication

There are three types of OSPF authentications--Null (Type 0), Simple Text (Type 1), and MD5 (Type 2). With Null authentication, routing exchanges over the network are not authenticated. In Simple Text authentication, the authentication type is the same for all routers that communicate using OSPF in a network. For MD5 authentication, configure a key and a key ID on each router. The router generates a message digest on the basis of the key, key ID, and OSPF packet, and adds it to the OSPF packet.

The authentication type can be configured on a per-interface basis or a per-area basis. Additionally, Interface and Area authentication can be used together. Area authentication is used for an area, and interface authentication is used for a specific interface in the area. If the Interface authentication type is different from the Area authentication type, the Interface authentication type overrides the Area authentication type. If the Authentication type is not specified for an interface, the Authentication type for the area is used. The authentication command descriptions contain details of each type of authentication.

In the example below, R1 and R2 are configured for both the interface and area authentications. The authentication type of interface eth1 on R1 and interface eth0 on R2 is MD5 mode, and is defined by the area authentication command; however, the authentication type of interface eth2 on R1 and interface eth1 on R2 is plain text mode, and is defined by the `ip ospf authentication` command. This interface command overrides the `area authentication` command.

Topology

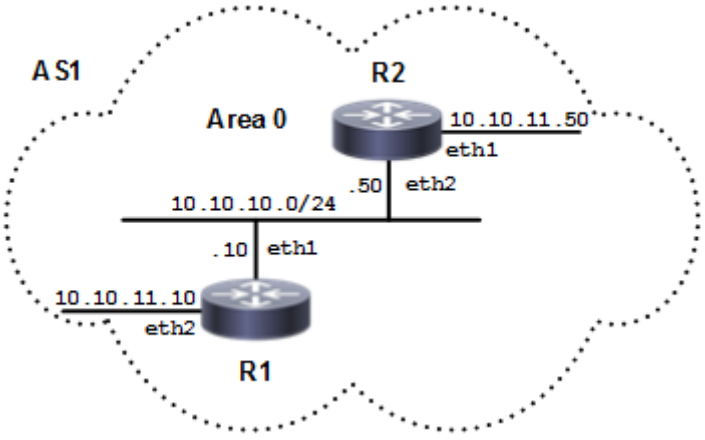


Figure 4-7: OSPF Authentication Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID 0 specifies the backbone area).
`(config-router)#area 0 authentication message-digest`	Enable MD5 authentication on area 0.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip ospf message-digest-key 1 md5 0 test`	Register the MD5 key test for OSPF authentication. The key ID is 1.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf authentication`	Enable the OSPF packet to use text authentication on the current interface (`eth2`).
`(config-if)#ip ospf authentication-key 0 test`	Specify an OSPF authentication password (`test`) for the neighboring routers.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID 0 specifies the backbone area).
`(config-router)#area 0 authentication message-digest`	Enable MD5 authentication on area 0.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf message-digest-key 1 md5 0 test`	Register MD5 key test for OSPF authentication. The key ID is 1.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip ospf authentication`	Enable the OSPF packet to use text authentication on the current interface (`eth1`).
`(config-if)#ip ospf authentication-key 0 test`	Specify an OSPF authentication password `test` for the neighboring routers.

Validation

R1

```
R1#sh running-config
!
no service password-encryption
!
hostname R1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
 ip address 10.10.10.10/24
 ip ospf message-digest-key 1 md5 0x293da85becc67703
!
interface eth2
 ip address 10.10.11.10/24
 ip ospf authentication
 ip ospf authentication-key 0x293da85becc67703
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 100
 area 0.0.0.0 authentication message-digest
 network 10.10.9.0/24 area 0.0.0.0
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.0
 network 10.10.12.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
```

```
 login
!
end


R1#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/DR         00:00:38    10.10.10.50     eth1
0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 10.10.11.50/24
 ip ospf authentication
 ip ospf authentication-key 0x293da85becc67703
!
interface eth2
 ip address 10.10.10.50/24
 ip ospf message-digest-key 1 md5 0x293da85becc67703
 ip ospf cost 100
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 100
 area 0.0.0.0 authentication message-digest
```

```
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end

R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:33    10.10.10.10     eth2
0
```

Multiple OSPF Instances

By using multiple OSPF instances, OSPF routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

To configure multiple OSPF instances, perform the following procedures referring to the topology diagram below:

1. Enable OSPF on an interface.
2. Enable multiple instances.
3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type or route-map options.

Topology

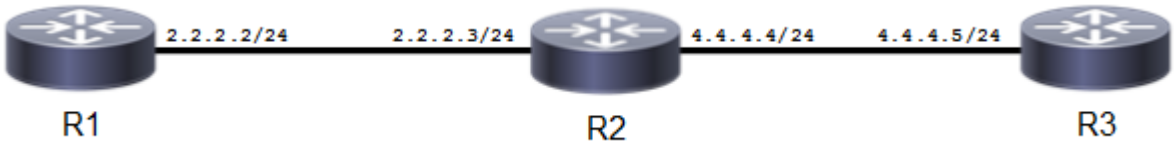


Figure 4-8: Multiple OSPF Instances

Enable Multiple OSPF Instances on a Router

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPF.

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip address 2.2.2.2/24`	Specify the IP address of the interface.
`(config-if)#no shutdown`	Activate the interface.

(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure an OSPF instance with an instance ID of 10.
(config-router)#router-id 5.5.5.5	Configure the router ID to use on this instance.
(config-router)#network 2.2.2.0/24 area 0	Advertise the network with the area ID.

R2

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ip address 2.2.2.3/24	Specify the IP address of the interface.
(config-if)#no shutdown	Activate the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure an OSPF instance with an instance ID of 10.
(config-router)#router-id 6.6.6.6	Configure the router ID to use on this instance.
(config-router)#network 2.2.2.0/24 area 0	Advertise the network with the area ID.
(config-router)#exit	Exit router mode.
(config)#interface eth2	Enter interface mode for eth2.
(config-if)#ip address 4.4.4.4/24	Configure the IP address.
(config-if)#no shutdown	Activate the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 15	Configure an OSPF instance with an instance ID of 15.
(config-router)#router-id 8.8.8.8	Configure the router ID to use on this instance.
(config-router)#network 4.4.4.0/24 area 0	Advertise the network with the area ID.

R3

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ip address 4.4.4.5/24	Configure the IP address.
(config-if)#no shutdown	Activate the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 15	Configure an OSPF instance with an instance ID of 15.
(config-router)#router-id 7.7.7.7	Configure the router ID to use on this instance.
(config-router)#network 4.4.4.0/24 area 0	Advertise the network with the area ID.

Validation

R1

```
R1#sh running-config
!
no service password-encryption
!
hostname R1
!
logging monitor 7
!
```

```
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
 ip address 2.2.2.2/24
!
interface eth2
 ip address 10.10.11.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 10
 ospf router-id 5.5.5.5
 network 2.2.2.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end

R1#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
6.6.6.6         1   Full/Backup     00:00:39   2.2.2.3       eth1
0

R1#sh ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 2.2.2.3/24
!
interface eth2
 ip address 4.4.4.4/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 10
 ospf router-id 6.6.6.6
 network 2.2.2.0/24 area 0.0.0.0

!
router ospf 15
 ospf router-id 8.8.8.8
 network 4.4.4.0/24 area 0.0.0.0
 no capability cspf
!
line con 0
 login
line vty 0 39
 login
!
end
```

```
R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
5.5.5.5         1   Full/DR        00:00:33    2.2.2.2       eth1
0

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
7.7.7.7         1   Full/Backup     00:00:31    4.4.4.5       eth2
0

R2#sh ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R3

```
R3#sh running-config
!
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.90/24
!
interface eth1
```

```
 ip address 4.4.4.5/24
!
interface eth2
 ip address 10.10.13.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 15
 ospf router-id 7.7.7.7
 network 4.4.4.0/24 area 0.0.0.0

!
line con 0
 login
line vty 0 39
 login
!
end

R3#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
8.8.8.8           1   Full/DR         00:00:30    4.4.4.4         eth1
0
```

Redistribute among Multiple Instances

In this example, routes of one instance are redistributed to another instance to enable ping from R1 to R3 or vice versa; and R2 redistributes routes from one instance to another.

R2

`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.
`(config-router)#redistribute ospf 10`	Redistribute instance `10` routes.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 10`	Configure an OSPF instance with instance ID `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID.
`(config-router)#redistribute ospf 15`	Redistribute instance `15` routes.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `10`.

Redistribute with the Metric Option

In this example, on R3, R1 and R2 have each other's routes with a metric of 100.

R2

`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.
`(config-router)#redistribute ospf 10 metric 100`	Redistribute instance `10` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 10`	Configure an OSPF instance with instance ID `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID.
`(config-router)#redistribute ospf 15 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `10`.

Redistribute with the Type Option

In this example, on R3, R1 has R3 routes as type 2, and R2 has R1 routes as type 1.

R2

`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.
`(config-router)#redistribute ospf 10 metric-type 1`	Redistribute instance `10` routes with metric-type `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 10`	Configure an OSPF instance with instance ID `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID.
`(config-router)#redistribute ospf 15 metric-type 2`	Redistribute instance `15` routes with type `2`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `10`.

Redistribute with the Route-Map Option

R2

`(config)#route-map 1 permit 10`	Enter route-map mode, specifying route-map ID.
`(config-route-map)#set metric 100`	Set metric value.
`(config-route-map)#set metric-type type-2`	Set metric-type.
`(config-route-map)#exit`	Exit route-map mode.

(config)#route-map 2 permit 10	Enter route-map mode, specifying route-map ID.
(config-route-map)#set metric 200	Set metric value.
(config-route-map)#set metric-type type-1	Set metric-type.
(config-route-map)#exit	Exit route-map mode.
(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 route-map 1	Redistribute instance 10 routes with route map 1.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 route-map 2	Redistribute instance 15 routes with route map 2.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Validation

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/DR         00:00:39    2.2.2.3         eth1
0

R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
5.5.5.5           1   Full/Backup     00:00:35    2.2.2.2         eth1
0

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
7.7.7.7           1   Full/Backup     00:00:36    4.4.4.5         eth2
0
R3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
8.8.8.8           1   Full/DR         00:00:40    4.4.4.4         eth2
0
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     2.2.2.0/24 is directly connected, eth1, 00:08:40
O E1  4.4.4.0/24 [110/201] via 2.2.2.3, eth1, 00:01:18
C     5.5.5.5/32 is directly connected, lo, 00:08:41
O E2  6.6.6.6/32 [110/20] via 2.2.2.3, eth1, 00:01:10
O E2  8.8.8.8/32 [110/20] via 2.2.2.3, eth1, 00:01:10
C     127.0.0.0/8 is directly connected, lo, 00:08:44
C     192.168.20.0/24 is directly connected, eth0, 00:08:40

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     2.2.2.0/24 is directly connected, eth1, 5d00h02m
C     4.4.4.0/24 is directly connected, eth2, 5d00h02m
C     6.6.6.6/32 is directly connected, lo, 4d23h59m
C     8.8.8.8/32 is directly connected, lo, 4d23h59m
C     127.0.0.0/8 is directly connected, lo, 5d00h09m
C     192.168.20.0/24 is directly connected, eth0, 5d00h08m

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O E2  2.2.2.0/24 [110/20] via 4.4.4.4, eth2, 00:02:45
C     4.4.4.0/24 is directly connected, eth2, 00:07:12
C     5.5.5.5/32 is directly connected, lo, 00:16:35
O E2  6.6.6.6/32 [110/20] via 4.4.4.4, eth2, 00:02:45
O E2  8.8.8.8/32 [110/20] via 4.4.4.4, eth2, 00:02:45
C     127.0.0.0/8 is directly connected, lo, 00:16:39
C     192.168.20.0/24 is directly connected, eth0, 00:15:36
```

```
Gateway of last resort is not set

#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0

R2#show route-map

route-map 1, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 100
    metric-type type-2
route-map 2, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 200
    metric-type type-1

R1#show ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
E1 4.4.4.0/24 [201] via 2.2.2.3, eth1
E2 6.6.6.6/32 [1/20] via 2.2.2.3, eth1
E2 8.8.8.8/32 [1/20] via 2.2.2.3, eth1
E2 192.168.20.0/24 [1/20] via 2.2.2.3, eth1

R2#show ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

```
R3#show ip ospf route

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

E2 2.2.2.0/24 [1/20] via 4.4.4.4, eth2
C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
E2 6.6.6.6/32 [1/20] via 4.4.4.4, eth2
E2 8.8.8.8/32 [1/20] via 4.4.4.4, eth2
E2 192.168.20.0/24 [1/20] via 4.4.4.4, eth2
```

Multiple OSPF Instances on Same Subnet

Multiple OSPF instances can be configured on the same subnet. The OSPF instance ID supports separate OSPFv2 protocol instances. With this feature, an adjacency is formed only if the received packet's instance ID is the same as the instance ID configured for that interface.

Topology

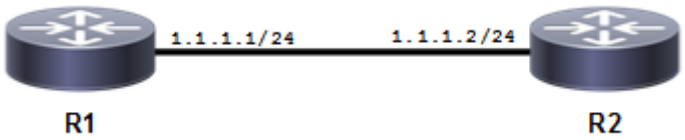


Figure 4-9: Multiple Instances on the Same Subnet

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#enable ext-ospf-multi-inst`	Enable multiple-instance capability.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of 1.
`(config-router)#network 1.1.1.0/24 area 0 instance-id 1`	Advertise the network in Area 0 with an instance ID of 1.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 2`	Configure an OSPF instance with an instance ID of 2.
`(config-router)#network 1.1.1.0/24 area 0 instance-id 2`	Advertise the network in Area 0 with an instance ID of 2.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#enable ext-ospf-multi-inst`	Enable multiple-instance capability.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of 1.
`(config-router)#network 1.1.1.0/24 area 0 instance-id 1`	Advertise the network in Area 0 with an instance ID of 1.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 2`	Configure an OSPF instance with an instance ID of 2.
`(config-router)#network 1.1.1.0/24 area 0 instance-id 2`	Advertise the network in Area 0 with an instance ID of 2.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

Validation

R1

```
R1#show ip ospf interface
eth1 is up, line protocol is up
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 7 sent 16, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 4 sent 12, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication

R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/Backup     00:00:35    1.1.1.2         eth1
1

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/Backup     00:00:33    1.1.1.2         eth1
2
```

R2

```
R2#sh ip ospf interface
eth1 is up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 17 sent 17, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 13 sent 14, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication

R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/DR        00:00:32    1.1.1.1         eth1
1

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
```

```
10.12.26.88      1   Full/DR         00:00:37    1.1.1.1       eth1
2
```

Multi-Area Adjacency Configuration

Multiple OSPF areas for a same subnet can be configured between two routers. In the diagram below, OSPF is enabled between R2 and R3 under area 0 and area 1, though there is only one link available between these two routers. Multi-area adjacency allows establishing adjacency on multiple areas between the Area Border Routers (ABRs). The specified interface of the ABR is associated with multiple areas.

Each multi-area-adjacency internally implements point-to-point functionality, once the adjacency reaches the FULL state. This point-to-point link provides a topological path for that area. Like a virtual link, there is no restriction for multi-area adjacency that the packets always go through the backbone.

Topology

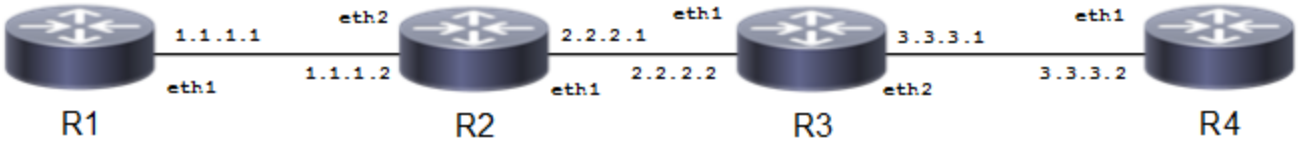


Figure 4-10: One Subnet with Multiple OSPF Areas

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of 1.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area 1.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of 1.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area 1.
`(config-router)#network 2.2.2.0/24 area 0`	Configure OSPF between R2 and R3 under area 0.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 2.2.2.1/24`	Configure IP address on the interface.
`(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.2`	Configure multi area adjacency.
`(config-if)#exit`	Exit interface mode.

R3

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 2.2.2.0/24 area 0`	Configure OSPF between R2 and R3 under area `0`.
`(config-router)#network 3.3.3.0/24 area 1`	Configure OSPF between R3 and R4 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/24`	Configure IP address on the interface.
`(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.1`	Configure multi area adjacency.
`(config-if)#exit`	Exit interface mode.

R4

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 3.3.3.0/24 area 1`	Configure OSPF between R3 and R4 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

Validation

R2

```
R2#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.2
  Internet Address 2.2.2.1/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.89, Network Type POINTTOPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 16 sent 53, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 10 sent 5
  LS-Ack received 3 sent 9, Discarded 0

R2#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
10.12.26.88      1   Full/DR        00:00:35   1.1.1.1       eth2
0
10.12.26.90      1   Full/Backup     00:00:33   2.2.2.2       eth1
0
10.12.26.90       1   Full/ -          00:00:35    2.2.2.2         eth1

R2#show ip ospf route

OSPF process 1:
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  1.1.1.0/24 [1] is directly connected, eth2, Area 0.0.0.1
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  3.3.3.0/24 [2] via 2.2.2.2, eth1, Area 0.0.0.1


R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
C       1.1.1.0/24 is directly connected, eth2
C       2.2.2.0/24 is directly connected, eth1
O       3.3.3.0/24 [110/2] via 2.2.2.2, eth1, 00:05:44
C       10.12.26.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

R3

```
R3#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.1
  Internet Address 2.2.2.2/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.90, Network Type POINTTOPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 41 sent 41, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 10
  LS-Ack received 8 sent 3, Discarded 0

R3#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
10.12.26.89      1   Full/DR        00:00:39    2.2.2.1       eth1
0
10.12.26.92      1   Full/Backup    00:00:36    3.3.3.2       eth2
0
10.12.26.89       1    Full/ -          00:00:30    2.2.2.1         eth1
R3#sh ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
O  1.1.1.0/24 [2] via 2.2.2.1, eth1, Area 0.0.0.1
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C  3.3.3.0/24 [1] is directly connected, eth2, Area 0.0.0.1

R3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
O       1.1.1.0/24 [110/2] via 2.2.2.1, eth1, 00:07:31
C       2.2.2.0/24 is directly connected, eth1
C       3.3.3.0/24 is directly connected, eth2
C       10.12.26.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

LSA Throttling

This section contains basic OSPF LSA throttling configuration examples.

The OSPF Link-State Advertisement (LSA) throttling feature provides a mechanism to dynamically slow down link-state advertisement (LSA) updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds, when the network is stable.

How OSPF LSA Throttling Works

The `timers throttle lsa all` command controls the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID.

The `timers lsa arrival` command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the `timers throttle lsa all` command.

Topology

The diagram shows the minimum configuration required to enable OSPF LSA Throttling Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

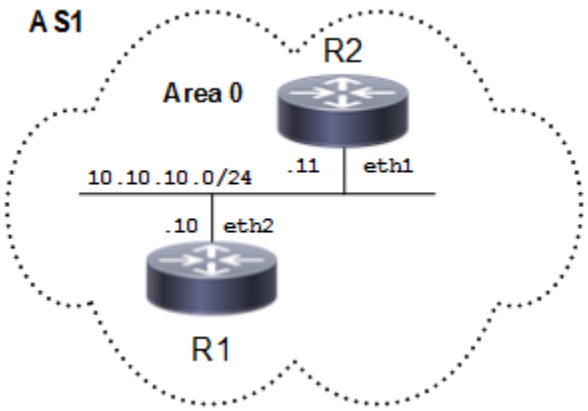


Figure 4-11: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#timers throttle lsa all 10000 20000 45000`	Configure LSA Throttling timers (Starting interval: <0-600000>, Min Hold Interval: <1-600000> and Max Wait Interval:< 1-600000>) in milliseconds. The Default value for corresponding timers are: Starting interval: 0, Min Hold Interval: 5 sec and Max Wait Interval: 5 sec.
`(config-router)#logging monitor 7`	Enable logging monitor globally.
`(config-router)#logging level ospf 7`	Enable logging level ospf globally.
`(config-router)#end`	Exit router mode

R2

`#configure terminal`	Enter configure mode.

`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

Validation

R1

Check the output of `show ip ospf` and verify the initial throttle delay, minimum hold time for LSA throttle and maximum wait time for LSA throttle.

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 11 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-8) | Total (8/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:10:12.807 ago
        SPF algorithm executed 5 times
        Number of LSA 7. Checksum 0x02c480
 Dste Staus: Disabled


#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID  Pri State       Dead Time  Address     Interface Instance ID
3.1.1.1      1   Full/Backup 00:00:34   10.10.10.11   eth1       0
```

```
#debug ospf database-timer rate-limit

#show debugging ospf
OSPF debugging status:
  OSPF rate limit timer events debugging is on
```

Here, we administratively shutdown and then bring up the loopback interface to generate Rate Limit Timer events for OSPF debugging to capture.

```
(config)#int lo
(config-if)#shutdown
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_DOWN_4]:
Received Link down for interface: lo
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : INFO : Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: with 10000 msec delay
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Loopback -> Down

(config-if)#no shutdown
2019 Mar 29 16:32:42.705 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_UP_4]:
Received Link up for  interface: lo
2019 Mar 29 16:32:42.705 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Down -> Loopback
2019 Mar 29 16:32:46.853 : OcNOS : OSPF : INFO : Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: expired
2019 Mar 29 16:32:46.853 : OcNOS : OSPF : INFO : For Next Instance of
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: generation wait 20000 msec


(config-if)#shutdown
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_DOWN_4]:
Received Link down for interface: lo
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : INFO : Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: with 12499 msec delay
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Loopback -> Down

(config-if)#no shutdown
2019 Mar 29 16:32:59.252 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_UP_4]:
Received Link up for  interface: lo
2019 Mar 29 16:32:59.252 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Down -> Loopback
2019 Mar 29 16:33:06.870 : OcNOS : OSPF : INFO : Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: expired
2019 Mar 29 16:33:06.870 : OcNOS : OSPF : INFO : For Next Instance of
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: generation wait 40000 msec
```

R2

Check the output of "`show ip ospf neighbor`" and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID  Pri  State     Dead Time   Address    Interface  Instance ID
1.1.1.1      1    Full/DR   00:00:33    10.10.10.10   eth1       0
```

Check the output of `show ip ospf database` and verify that LSA (router LSA in this example) is updated according to the configured LSA throttling timers configured on its neighbor.

```
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          373     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           71     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          375     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          372     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          373     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          372     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          373     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          378     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           76     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          380     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router       Age      Seq#      CkSum Opaque ID
1.0.0.1         3.1.1.1          377     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          378     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          377     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          378     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)
```

```
Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          380     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           78     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          382     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          379     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          380     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          379     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          380     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          381     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           79     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          383     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          380     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          381     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          380     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          381     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          382     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           80     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          384     0x80000001 0x18e5
```

```
                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          381     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          382     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          381     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          382     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          383     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           81     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          385     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          382     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          383     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          382     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          383     0x80000001 0x566c 8
```

Configure OSPF LSA Arrival Timers

The diagram shows the minimum configuration required to enable OSPF Minimum LSA Arrival Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

Topology

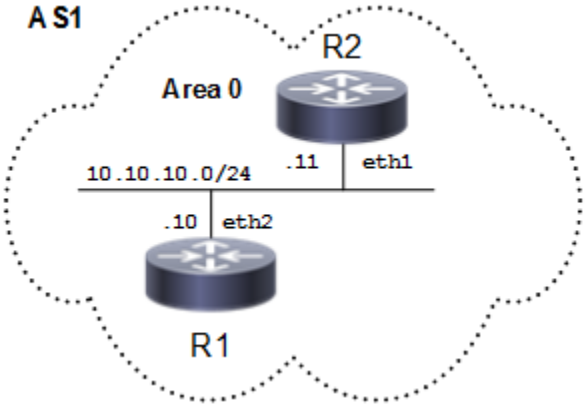


Figure 4-12: Basic OSPF Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#end`	Exit router mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.
`(config-router)#timers lsa arrival 100000`	Configure Minimum LSA Arrival timers (Minimum LSA arrival Interval:< 0-600000>) in milliseconds. The Default value for Minimum LSA Arrival timer is: 1 sec.

Validation

R1

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer by default is set to 1 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 11 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-8) | Total (8/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:10:12.807 ago
        SPF algorithm executed 5 times
        Number of LSA 7. Checksum 0x02c480
 Dste Staus: Disabled

#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
3.1.1.1          1   Full/Backup      00:00:34    10.10.10.11     eth1
```

R2

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer is set to 100 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 3.1.1.1
 Process uptime is 23 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 100 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 10
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-9) | Total (9/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:22:12.911 ago
        SPF algorithm executed 4 times
        Number of LSA 7. Checksum 0x02c281
 Dste Staus: Disabled
```

Check the output of show ip ospf neighbor and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
1.1.1.1         1   Full/DR        00:00:35   10.10.10.10    eth1
0
```

Check the output of “show ip ospf database” and verify that LSA is accepted only after a time difference of 100 sec between two consecutive LSAs.

```
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)
```

```
Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1131     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          829     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1133     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1130     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1131     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1130     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1131     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1132     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          831     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1134     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1131     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1132     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1131     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1132     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1133     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          831     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1135     0x80000001 0x18e5
```

```
                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1132     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1133     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1132     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1133     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1134     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          832     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1136     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1133     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1134     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1133     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1134     0x80000001 0x566c 8
#
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1135     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          834     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1137     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1134     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1135     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1134     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1135     0x80000001 0x566c 8


#show ip ospf database
```

```
            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1136     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          834     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1138     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1135     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1136     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1135     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1136     0x80000001 0x566c 8
```

Loop-Free Alternate Fast Reroute

This section contains basic OSPF Loop-Free Alternate Fast Reroute (LFA-FRR) configuration examples.

Overview

The goal of (LFA-FRR) is to reduce failure reaction time to 10s of milliseconds by using a pre-computed alternate next-hop in the event that the currently selected primary next-hop fails, so that the alternate can be rapidly used when the failure is detected. A network with this feature experiences less traffic loss and less micro-looping of packets than a network without LFA-FRR.

After enabling LFA-FRR on routers, routers calculate a backup path for each primary path to reach the destination.The backup path is calculated based on the attributes such as node protecting, link protecting, broadcast-link protecting and secondary path.

OSPF LFA and ISIS LFA along with MPLS is not supported. Do not configure OSPF LFA or ISIS LFA, if MPLS is configured or vice-versa.

Topology

The diagram shows the configuration required to enable the OSPF LFA feature.

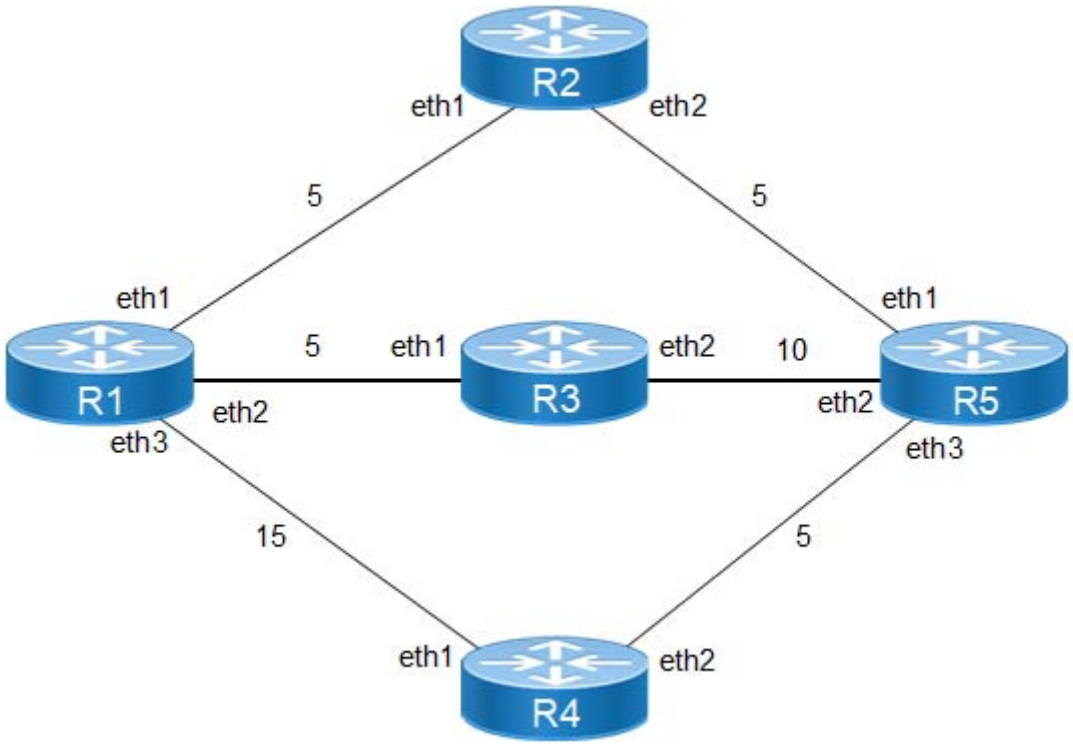


Figure 4-13: Basic OSPF-LFA Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 30.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process and specify the Process ID (1).
`(config-router)#network 10.1.1.0/24 area 0`	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 20.1.1.0/24 area 0`	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 30.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).

(config-router)#fast-reroute keep-all- paths	Configure LFA-FRR to calculate the available backup path.
(config-router)#end	Exit router mode.

R2

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.1.1.1/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#end	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.1.1.1/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#end	Exit router mode.

R4

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 30.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 30.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#end`	Exit router mode.

R5

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 40.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 50.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 40.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 50.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#end`	Exit router mode.

Validation

R1

Check OSPF neighborship.

```
#show ip ospf neighbor
OSPF Process 100 VRF (default)
Neighbor ID     Pri   State           Dead Time   Address  Interface Intance
ID
2.2.2.2           1   Full/DR         00:00:33    10.1.1.2     eth1  0
3.3.3.3           1   Full/DR         00:00:33    20.1.1.2     eth2  0
4.4.4.4           1   Full/DR         00:00:39    30.1.1.2     eth2  0
#
Check the OSPF route installation and LFA-FRR backup path for the primary
path.
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1
C     20.1.1.0/24 is directly connected, eth2
C 30.1.1.0/24 is directly connected, eth3
O     40.1.1.0/24 [110/10] via 10.1.1.2, eth1, 00:16:43
O     50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:16:43
O IA  60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:16:43
O E2  70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:16:43
O E2 80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:16:43
C 127.0.0.0/8 is directly connected, lo
C 192.168.100.0/24 is directly connected, eth0
Gateway of last resort is not set

Not mandatory that for all primary path, there exists an LFA backup path only
if inequality equation satisfies according to attributes configured on
routers, backup path will be calculated.
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1

O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:00:34
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
```

```
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2

Not mandatory that for all primary path, there exists an LFA backup path only
if inequality equation satisfies according to attributes configured on
routers, backup path will be calculated.
```

To prohibit an interface from being used as a repair path, disable fast reroute calculation on the interface.

```
(config)#int eth3
(config-if)#ip ospf fast-reroute per-prefix candidate disable
(config-if)#end
```

Verify that the `eth3` interface is not used for backup path calculation.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
O       10.1.1.0/24 [110/10] via 20.1.1.1, eth1, 00:34:04
C       20.1.1.0/24 is directly connected, eth1
O       30.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:34:04
O       40.1.1.0/24 [110/15] via 20.1.1.1, eth1, 00:34:04
                    [110/15] via 50.1.1.2, eth2, 00:34:04
C       50.1.1.0/24 is directly connected, eth2
O IA    60.1.1.0/24 [110/15] via 50.1.1.2, eth2, 01:08:29
O E2    70.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:34:03
O E2    80.1.1.0/24 [110/20] via 50.1.1.2, eth2, 01:11:17
C       127.0.0.0/8 is directly connected, lo
C       192.168.100.0/24 is directly connected, eth0
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
O       10.1.1.0/24 [110/10] via 20.1.1.1, eth1, 00:00:34
                    [FRR-NH] via 50.1.1.2, eth2

O       30.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:00:34
                    [FRR-NH] via 50.1.1.2, eth2

O       60.1.1.0/24 [110/15] via 50.1.1.2, eth2, 00:02:27
                    [FRR-NH] via 20.1.1.1, eth1

O       70.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:02:27
```

```
                        [FRR-NH] via 50.1.1.2, eth2

    O       80.1.1.0/24 [110/20] via 50.1.1.2, eth2, 00:02:27
```

Note: Now the LFA backup paths have been changed, `eth3` is not used.

LFA Tie-Breaker

Based on the index values configured, if inequalities are satisfied, protections will be provided:

- Lower the index will have the highest priority, the path which provides protection with highest priority will be selected. If there are multiple paths providing the highest priority protection, then we will check which path provides the protection which has 2nd highest priority and so on.
- If all the paths provide same priority, then the LFA route is chosen on the basis of path cost.
- If none of the paths provides the protection with highest priority, then we will see which path provides the 2nd highest priority and so on.

```
config)#router ospf 100
(config-router)#fast-reroute tie-break ?
broadcast-interface-disjoint  Prefer broadcast link protecting backup path

                              *Default value is 70

downstream-path               Prefer backup path from downstream

                              *Default value is 90

interface-disjoint            Prefer link protecting backup path

                              *Default value is 60

node-protecting               Prefer node protecting backup path

                              *Default value is 30

primary-path                  Prefer backup path from ECMP set

                              *Default value is 20

secondary-path                Prefer non-ECMP backup path

                              *Default value is 255
(config-router)#fast-reroute tie-break broadcast-interface-disjoint index 1
(config-router)#fast-reroute tie-break node-protecting index 2
```

Verify show ip route and show ip route fast-reroute for backup path calculated according to attributes configured above.

```
    #show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
    OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
    external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1
C     20.1.1.0/24 is directly connected, eth2
C 30.1.1.0/24 is directly connected, eth3
O     40.1.1.0/24 [110/10] via 10.1.1.2, eth1, 01:07:26
O     50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 01:07:26
O IA  60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 01:07:26
O E2  70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 01:07:26
O E2 80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 01:07:26
C 127.0.0.0/8 is directly connected, lo
C 192.168.100.0/24 is directly connected, eth0

Gateway of last resort is not set
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"

O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1

O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2

#show ip ospf route fast-reroute

OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, ID - Interface Disjoint,
       NP - Node Protecting, BID - Broadcast Interface Disjoint

O  50.1.1.0/24 [15] via 20.1.1.1, eth2, Area 0.0.0.0
                       Backup path:
                        via 10.1.1.2, eth1, Area 0.0.0.0
                       Attributes: Metric: [20] ,LP ,NP, BP
O  60.1.1.0/24 [15] via 10.1.1.2, eth1, Area 0.0.0.0
                       Backup path:
                        via 20.1.1.2, eth2, Area 0.0.0.0
```

```
                          Attributes: Metric: [15] ,LP ,NP,BP
O  70.1.1.0/24 [20] via 30.1.1.2, eth3, Area 0.0.0.0
                          Backup path:
                           via 10.1.1.2, eth1, Area 0.0.0.0
                          Attributes: Metric: [20] ,LP ,NP,BP
O  80.1.1.0/24 [20] via 10.1.1.2, eth1, Area 0.0.0.0
                          Backup path:
                           via 20.1.1.2, eth2, Area 0.0.0.0
                          Attributes: Metric: [20] ,LP,NP,BP
```

LFA Termination

A router MUST limit the amount of time an alternate next-hop is used after the primary next-hop has become unavailable. This ensures that the router will start using the new primary next-hops.

LFA termination avoids a micro looping in topology, when particular network goes down, LFA backup path will be installed and if termination interval is configured, LFA backup will be still used till the interval and it is used in order to verify new primary path is loop free.

R1

Configure termination interval on R1 in router mode:

`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#fast-reroute terminate-hold-on interval 100000`	Configure LFA termination interval
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

If you check “show ip ospf” you can see the configured termination-hold on interval value along with ospf output:

```
#show ip ospf
IPFRR per-prefix tiebreakers:
    Name                              Index
    Primary path                      20
    Node Protecting                   30
    Interface disjoint                60
    Broadcast interface disjoint      70
    Secondary path                    255
 LFA termination hold-on timer : 100 secs 0 msecs

#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1
```

```
O       60.1.1.0/24 [110/15 via 10.1.1.2, eth1, 00:00:34
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2
```

Shut down one of the primary nexthops, here eth2 of rtr1:

(config)#interface eth2	Enter interface mode.
(config-if)#shutdown	Shutdown the interface
(config-if)#exit	Exit interface mode
(config-if)#exit	Exit interface mode.

```
    #show ip route fast-reroute
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
    area ,p - stale info
           * - candidate default

    IP Route Table for VRF "default"
    O       50.1.1.0/24 [110/15] via 20.1.1.2, eth1, 00:00:34  <<<eth1 which was
    back-up path before got  installed as new primary path
                        [FRR-NH] via 30.1.1.2, eth3

    O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:00:34
                        [FRR-NH] via 30.1.1.2, eth3

    O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                        [FRR-NH] via 10.1.1.2, eth1

    O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                        [FRR-NH] via 30.1.1.2, eth3
```

Loop-Free Alternate (LFA) ECMP PATH

This section contains configurations for OSPF LFA ECMP which provides LFA/alternate path from primary ECMP path set or non-primary/non-ECMP path set which improve convergence after a primary path failure occur in network.

Overview

With ECMP, a prefix has multiple primary paths to forward traffic. When a particular primary path fails, the other primary paths are not guaranteed to provide protection against the failure scenario. As part of LFA ECMP, alternate paths are determined for each primary path separately. The selected alternate path can be either one of the primary path from the set of ECMP or a loop-free non-ECMP if available.

In OSPF, by default the LFA algorithm tries to find loop free node protecting alternate from the set of existing primary next-hops. If no loop free node-protecting alternate is available, the LFA algorithm tries to find link-protecting alternate

from the set of existing primary next-hops. If no loop-free node-protecting and link-protecting alternate is available, then the LFA algorithm should select a loop-free link-protecting from the non-ECMP next-hops.

Topology

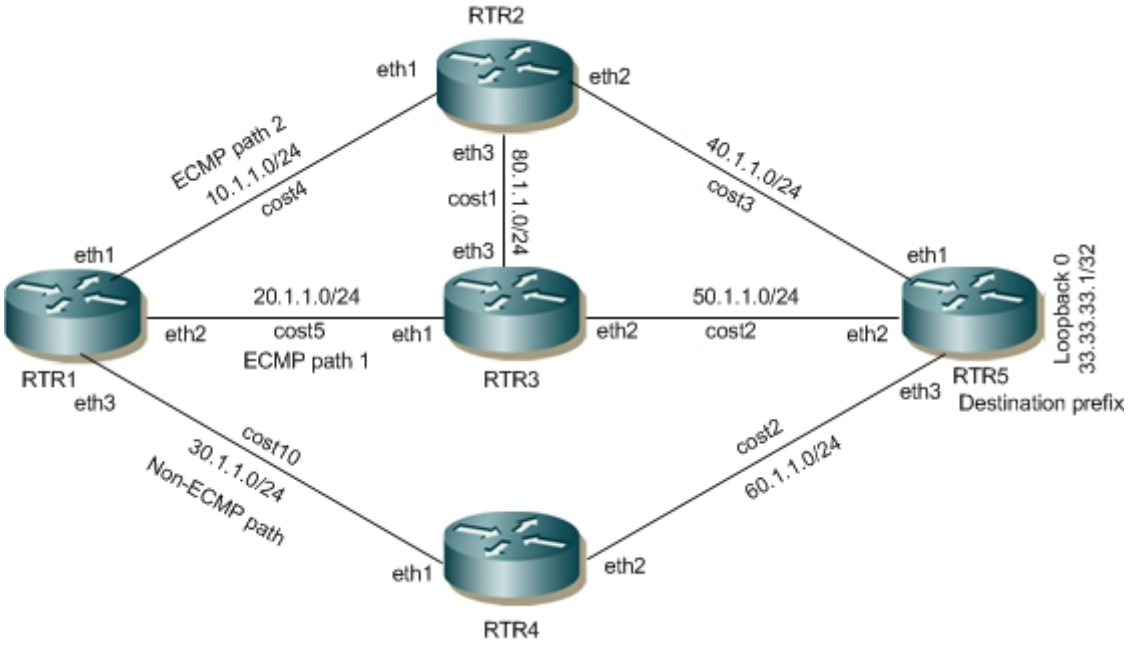


Figure 4-14: OSPF-LFA_ECMP

Configuring OSPF LFA ECMP

Configuration Part 1: with default LFA configuration where primary path priority higher than Secondary-path (non-ECMP) and LFA selection happen within primary ECMP path

RTR1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip ospf cost 4`	Assign cost to interface
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Assign IP address.
`(config-if)#ip ospf cost 5`	Assign cost to interface
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ip address 30.1.1.1/24`	Assign IP address.
`(config-if)#ip ospf cost 10`	Assign cost to interface
`(config-if)#exit`	Exit interface mode.

(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#ospf router-id 1.1.1.1	Configure router-id as 1.1.1.1
(config-router)#bfd all-interfaces	Enable BFD over ospf for all ospf enabled interfaces
(config-router)#network 10.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 20.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 30.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#fast-reroute keep-all-paths	Configure LFA-FRR to calculate the available backup path.
(config-router)#end	Exit router mode.

RTR2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure the IP address of the interface.
(config-if)#ip ospf cost 4	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 40.1.1.1/24	Assign IP address.
(config-if)#ip ospf cost 3	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 80.1.1.1/24	Assign IP address.
(config-if)#ip ospf cost 1	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#ospf router-id 2.2.2.2	Configure router-id.
(config-router)#bfd all-interfaces	Enable BFD over ospf for all ospf enabled interfaces
(config-router)#network 10.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 40.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 80.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#end	Exit router mode.

RTR3

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure the IP address of the interface.

(config-if)#ip ospf cost 5	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 50.1.1.1/24	Assign IP address.
(config-if)#ip ospf cost 2	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 80.1.1.2/24	Assign IP address.
(config-if)#ip ospf cost 1	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#ospf router-id 3.3.3.3	Configure router-id.
(config-router)#bfd all-interfaces	Enable BFD over ospf for all ospf enabled interfaces
(config-router)#network 20.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 50.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 80.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#end	Exit router mode.

RTR4

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 30.1.1.2/24	Configure the IP address of the interface.
(config-if)#ip ospf cost 10	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 60.1.1.1/24	Assign IP address.
(config-if)#ip ospf cost 2	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#ospf router-id 4.4.4.4	Configure router-id.
(config-router)#bfd all-interfaces	Enable BFD over ospf for all ospf enabled interfaces
(config-router)#network 30.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 60.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#end	Exit router mode.

RTR5

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 33.33.33.1/32	Assign IP address.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 40.1.1.2/24	Configure the IP address of the interface.
(config-if)#ip ospf cost 3	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 50.1.1.2/24	Assign IP address.
(config-if)#ip ospf cost 2	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 60.1.1.2/24	Assign IP address.
(config-if)#ip ospf cost 2	Assign cost to interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#ospf router-id 5.5.5.5	Configure router-id.
(config-router)#bfd all-interfaces	Enable BFD over ospf for all ospf enabled interfaces
(config-router)#network 40.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 50.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 60.1.1.0/24 area 0	Configure OSPF network for area 0.
(config-router)#network 33.33.33.1/32 area 0	Configure OSPF network for area 0.
(config-router)#end	Exit router mode.

Validation

Validation Part 1: LFA selected from primary ECMP path set

RTR1

```
#show ip ospf route fast-reroute

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, ID - Interface Disjoint,
       NP - Node Protecting, BID - Broadcast Interface Disjoint
```

```
O  33.33.33.1/32 [17] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                            via 20.1.1.2, eth2, Area 0.0.0.0
                           Attributes: Metric: [17] ,P ,NP
                      via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                            via 10.1.1.2, eth1, Area 0.0.0.0
                           Attributes: Metric: [17] ,P ,ID
O  40.1.1.0/24 [7] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [15] ,SP ,NP
O  50.1.1.0/24 [7] via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                         via 10.1.1.2, eth1, Area 0.0.0.0
                        Attributes: Metric: [7] ,P ,ID
                    via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                         via 20.1.1.2, eth2, Area 0.0.0.0
                        Attributes: Metric: [7] ,P ,NP
O  60.1.1.0/24 [9] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                         via 20.1.1.2, eth2, Area 0.0.0.0
                        Attributes: Metric: [9] ,P ,NP
                    via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                         via 10.1.1.2, eth1, Area 0.0.0.0
                        Attributes: Metric: [9] ,P ,ID
O  80.1.1.0/24 [5] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                         via 20.1.1.2, eth2, Area 0.0.0.0
                        Attributes: Metric: [6] ,SP ,NP

#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter  area, T - FRR nhp,p - stale info
       * - candidate default

IP Route Table for VRF "default"
O       33.33.33.1/32 [110/17] via 20.1.1.2, eth2, 00:00:44
                       [FRR-NH] via 10.1.1.2, eth1

                       [110/17] via 10.1.1.2, eth1
                       [FRR-NH] via 20.1.1.2, eth2

O       40.1.1.0/24 [110/7] via 10.1.1.2, eth1, 00:01:46
                    [FRR-NH] via 30.1.1.2, eth3

O       50.1.1.0/24 [110/7] via 10.1.1.2, eth1, 00:01:34
                    [FRR-NH] via 20.1.1.2, eth2

                    [110/7] via 20.1.1.2, eth2
```

```
                      [FRR-NH] via 10.1.1.2, eth1

O        60.1.1.0/24 [110/9] via 20.1.1.2, eth2, 00:01:34
                     [FRR-NH] via 10.1.1.2, eth1

                     [110/9] via 10.1.1.2, eth1
                     [FRR-NH] via 20.1.1.2, eth2

O        80.1.1.0/24 [110/5] via 10.1.1.2, eth1, 00:01:46
                     [FRR-NH] via 20.1.1.2, eth2


#show ip ospf route 33.33.33.1

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, ID - Interface Disjoint,
       NP - Node Protecting, BID - Broadcast Interface Disjoint

O  33.33.33.1/32 [17] via 10.1.1.2, eth1, Area 0.0.0.0
                      via 20.1.1.2, eth2, Area 0.0.0.0

#show ip route 33.33.33.1
Routing entry for 33.33.33.1/32
  Known via "ospf", distance 110, metric 17,  External Route Tag: 0, best
  Last update 00:00:40 ago
  * 20.1.1.2, via eth2
  * 10.1.1.2, via eth1
```

Configuration Part 2: with non-ECMP tiebreaker configured where secondary-path priority higher than primary (ECMP) path

Configure below configuration with config's shown in Part1:

RTR1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Enter Router OSPF mode.
`(config-router)#fast-reroute tie-break secondary-path index 5`	Configure LFA tiebreaker for LFA to be calculate from non-ecmp path set if available (this is user defined to decide the priority to select between ecmp/non-ecmp set)
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

Validation Part 2: LFA selected from non-ecmp path for each primary ecmp path

RTR1

```
#show ip ospf route fast-reroute

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, ID - Interface Disjoint,
       NP - Node Protecting, BID - Broadcast Interface Disjoint

O  33.33.33.1/32 [17] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                            via 30.1.1.2, eth3, Area 0.0.0.0
                           Attributes: Metric: [22] ,SP ,NP
                      via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                            via 30.1.1.2, eth3, Area 0.0.0.0
                           Attributes: Metric: [22] ,SP ,NP
O  40.1.1.0/24 [7] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [15] ,SP ,NP
O  50.1.1.0/24 [7] via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [14] ,SP ,NP
                   via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [14] ,SP ,NP
O  60.1.1.0/24 [9] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [12] ,SP ,NP
                   via 20.1.1.2, eth2, Area 0.0.0.0
                        Backup path:
                          via 30.1.1.2, eth3, Area 0.0.0.0
                         Attributes: Metric: [12] ,SP ,NP
O  80.1.1.0/24 [5] via 10.1.1.2, eth1, Area 0.0.0.0
                        Backup path:
                         via 20.1.1.2, eth2, Area 0.0.0.0
                        Attributes: Metric: [6] ,SP ,NP

#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area , T - FRR nhp,p - stale info
       * - candidate default

IP Route Table for VRF "default"
O       33.33.33.1/32 [110/17] via 20.1.1.2, eth2, 00:00:36
                       [FRR-NH] via 30.1.1.2, eth3

                       [110/17] via 10.1.1.2, eth1
                       [FRR-NH] via 30.1.1.2, eth3

O       40.1.1.0/24 [110/7] via 10.1.1.2, eth1, 00:01:38
                     [FRR-NH] via 30.1.1.2, eth3
```

```
O        50.1.1.0/24 [110/7] via 10.1.1.2, eth1, 00:01:26
                     [FRR-NH] via 30.1.1.2, eth3

                     [110/7] via 20.1.1.2, eth2
                     [FRR-NH] via 30.1.1.2, eth3

O        60.1.1.0/24 [110/9] via 20.1.1.2, eth2, 00:01:26
                     [FRR-NH] via 30.1.1.2, eth3

                     [110/9] via 10.1.1.2, eth1
                     [FRR-NH] via 30.1.1.2, eth3

O        80.1.1.0/24 [110/5] via 10.1.1.2, eth1, 00:01:38
```

[FRR-NH] via 20.1.1.2, eth2

CHAPTER 5 OSPFv3

This chapter contains basic OSPFv3 configuration examples.

Enable OSPFv3 on an Interface

This example shows the minimum configuration required for enabling OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to the network 3ffe:10::/64. After enabling OSPFv3 on an interface, create a routing instance, and specify the Router ID.

Note: You must explicitly specify a Router ID for the OSPFv3 process to be activated.

Topology

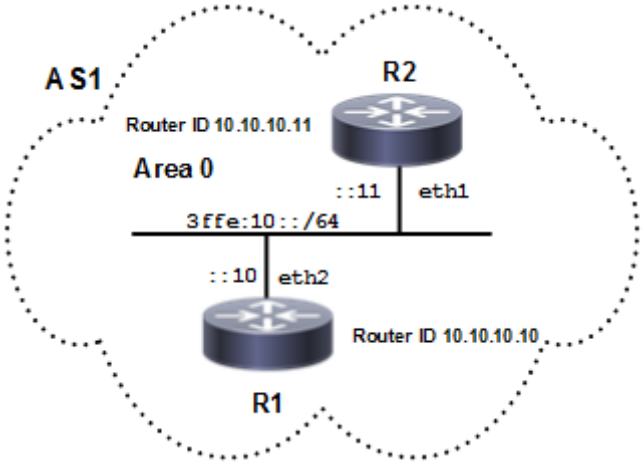


Figure 5-15: Basic OSPFv3 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `0`.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.

`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).

Validation

R1

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.11       1   Full/Backup     00:00:35    eth2       0

#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      164       0x80000001 0xf3c6      1
0.0.0.3         10.10.10.11      106       0x80000001 0xd973      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       94       0x80000003 0xb2f0      1
0.0.0.0         10.10.10.11       95       0x80000003 0x9e05      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       94       0x80000001 0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10       93       0x80000001 0xc35d      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       94       0x80000002 0x3504
0.0.0.3         10.10.10.11       95       0x80000002 0x6bcc

#show ipv6 ospfv3 topology
```

```
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10             --
10.10.10.11             1          10.10.10.11          eth2
```

R2

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:31    eth1       0

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      341       0x80000001 0xf3c6      1
0.0.0.3         10.10.10.11      281       0x80000001 0xd973      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      271       0x80000003 0xb2f0      1
0.0.0.0         10.10.10.11      270       0x80000003 0x9e05      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      271       0x80000001 0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10      270       0x80000001 0xc35d      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      271       0x80000002 0x3504
0.0.0.3         10.10.10.11      270       0x80000002 0x6bcc


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
```

```
10.10.10.10             1          10.10.10.10          eth1
10.10.10.11             --
```

Set Priority

This example shows how to set priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured with a priority of 10; this is higher than the default priority (default priority is 1) set for R1 and R2. This makes R3 the DR.

Topology

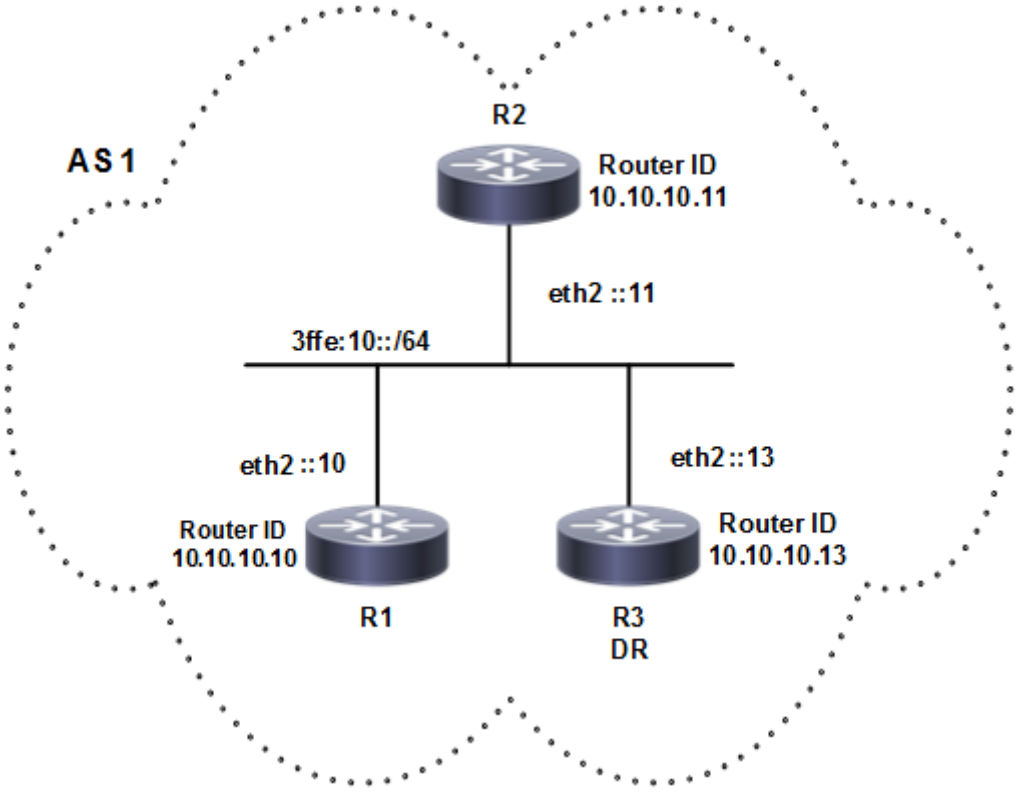


Figure 5-16: OSPFv3 Set Priority

R3

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.13`	Specify a Router ID (`10.10.10.13`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).
`(config-if)#ipv6 ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID (`10.10.10.10`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).

R2

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).

Validation

R1

```
rtr1#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.10.10.11       1   Full/DROther    00:00:37    eth2       0
10.10.10.13      10   Full/DR         00:00:37    eth2       0

rtr1#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum Prefix
0.0.0.4         10.10.10.10      398       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11       71       0x80000001 0x4768      1
0.0.0.4         10.10.10.13      611       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       49       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11       50       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13       61       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
```

```
0.0.0.4         10.10.10.13       61       0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13       60       0x80000002 0xd940      1  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       49       0x80000003 0x75bf
0.0.0.4         10.10.10.11       50       0x80000004 0x9f92
0.0.0.4         10.10.10.13       61       0x80000003 0xf935


rtr1#show ipv6 ospfv3 topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            --
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            1          10.10.10.13          eth2
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.10.10.10       1   Full/Backup     00:00:31    eth2       0
10.10.10.13      10   Full/DR         00:00:39    eth2       0

R2#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      525       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11      194       0x80000001 0x4768      1
0.0.0.4         10.10.10.13      736       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      175       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11      174       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13      186       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13      186       0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13      185       0x80000002 0xd940      1  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      175       0x80000003 0x75bf
0.0.0.4         10.10.10.11      174       0x80000004 0x9f92
0.0.0.4         10.10.10.13      186       0x80000003 0xf935

R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            --
10.10.10.13            1          10.10.10.13          eth2
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/Backup     00:00:38    eth2       0
10.10.10.11       1   Full/DROther    00:00:29    eth2       0

R3#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.13) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      658       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11      329       0x80000001 0x4768      1
0.0.0.4         10.10.10.13      869       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      309       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11      309       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13      319       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13      319       0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13      318       0x80000002 0xd940      1  Network-
LSA
```

```
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age         Seq#       CkSum
0.0.0.4         10.10.10.10      309        0x80000003 0x75bf
0.0.0.4         10.10.10.11      309        0x80000004 0x9f92
0.0.0.4         10.10.10.13      319        0x80000003 0xf935

R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            --
```

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, interface eth2 is in Area 0, and interface eth1 is in Area 1.

Topology

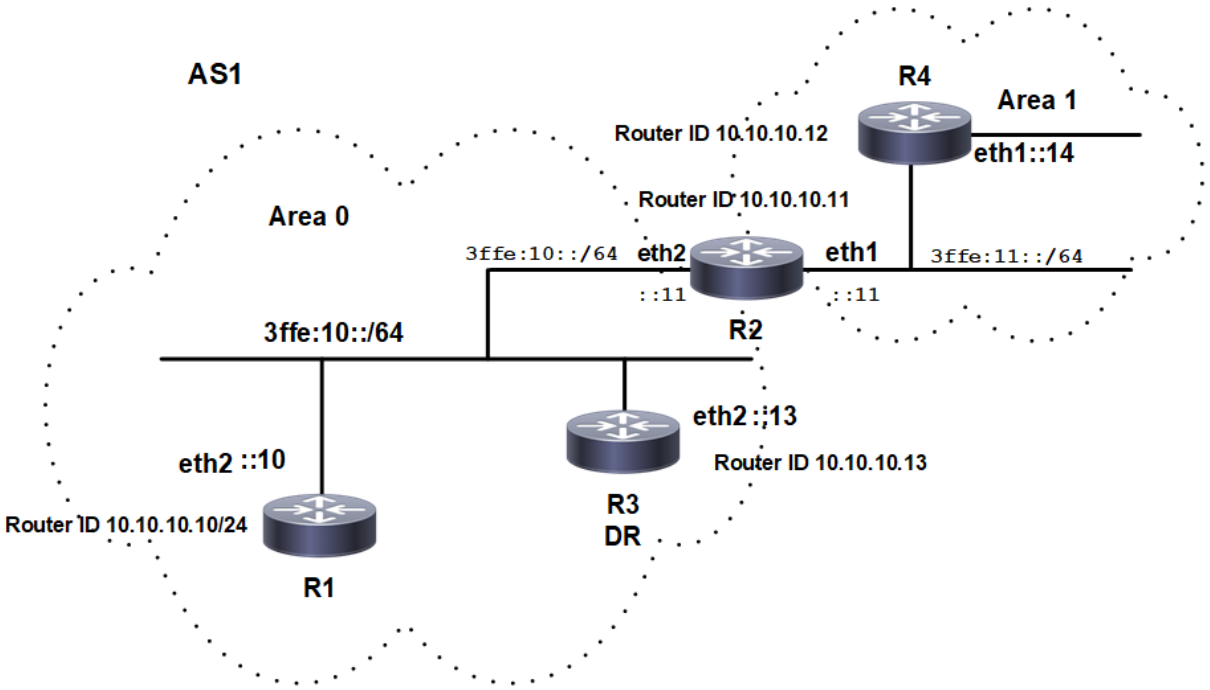


Figure 5-17: OSPFv3 Area Border Router

Configuration

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on the other interface, and assign the other Area ID (`1`).

R4

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.12`	Specify a Router ID (10.10.10.12) for the OSPFv3 routing process.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on the other interface, and assign the other Area ID (1).

Validation

R2

```
R2#show ipv6 ospf neighbor

Total number of full neighbors: 3
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.12       1   Full/Backup     00:00:32    eth1       0
10.10.10.10       1   Full/Backup     00:00:36    eth2       0
10.10.10.13      10   Full/DR         00:00:32    eth2       0
R2#

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.11      945       0x80000001 0x9d7f      1
0.0.0.3         10.10.10.12      797       0x80000001 0x271c      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10     1766       0x80000002 0x9a8b      1
0.0.0.4         10.10.10.11     1719       0x80000002 0x3fb0      1
0.0.0.4         10.10.10.13        6       0x80000004 0xd7e9      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10     1703       0x80000005 0xf0ad      1
0.0.0.0         10.10.10.11      945       0x80000006 0xebaf      1
0.0.0.0         10.10.10.13     1708       0x80000005 0xdebc      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13     1708       0x80000003 0xa4b1

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11      945       0x80000001 0xdc9f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13     1708       0x80000003 0xd741      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10     1703       0x80000004 0x4ef9
0.0.0.4         10.10.10.11     1704       0x80000004 0x7acb
0.0.0.4         10.10.10.13     1708       0x80000004 0xd26f

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.11      785       0x80000003 0xa5fc      1
0.0.0.0         10.10.10.12      785       0x80000003 0x9c06      1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.11      785       0x80000001 0x1672
```

```
                Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11      940       0x80000002 0xccaf

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.11      784       0x80000001 0xd747      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.11      785       0x80000002 0x70da
0.0.0.3         10.10.10.12      785       0x80000002 0x0146

R2#

R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11         B  --
10.10.10.13            1          10.10.10.13          eth2

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.11         B  --
10.10.10.12            1          10.10.10.12          eth1

R2#

R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:09:54
C      3ffe:10::/64 via ::, eth2, 01:06:27
C      3ffe:11::/64 via ::, eth1, 00:21:16 R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:10::/64                                       1
     directly connected, eth2, Area 0.0.0.0
C  3ffe:11::/64                                       1
     directly connected, eth1, Area 0.0.0.1
R2#


C      fe80::/64 via ::, eth9, 01:09:54
R2#
```

R1

```
R1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:27:52
C      3ffe:10::/64 via ::, eth2, 01:25:13
O IA   3ffe:11::/64 [110/2] via fe80::5054:ff:fe3d:e317, eth2, 00:36:07
C      fe80::/64 via ::, eth9, 01:27:52
R1#
```

R3

```
R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:26:53
C      3ffe:10::/64 via ::, eth2, 01:23:21
O IA   3ffe:11::/64 [110/2] via fe80::5054:ff:fe3d:e317, eth2, 00:34:39
C      fe80::/64 via ::, eth9, 01:26:53
R3#
```

R4

```
R4#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
```

```
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 00:47:25
O IA    3ffe:10::/64 [110/2] via fe80::5054:ff:fe0e:46b7, eth1, 00:30:12
C       3ffe:11::/64 via ::, eth1, 00:36:23
C       fe80::/64 via ::, eth9, 00:47:25
R4#
```

Redistribute Routes into OSPFv3

In this example, the BGP routes are imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

Topology

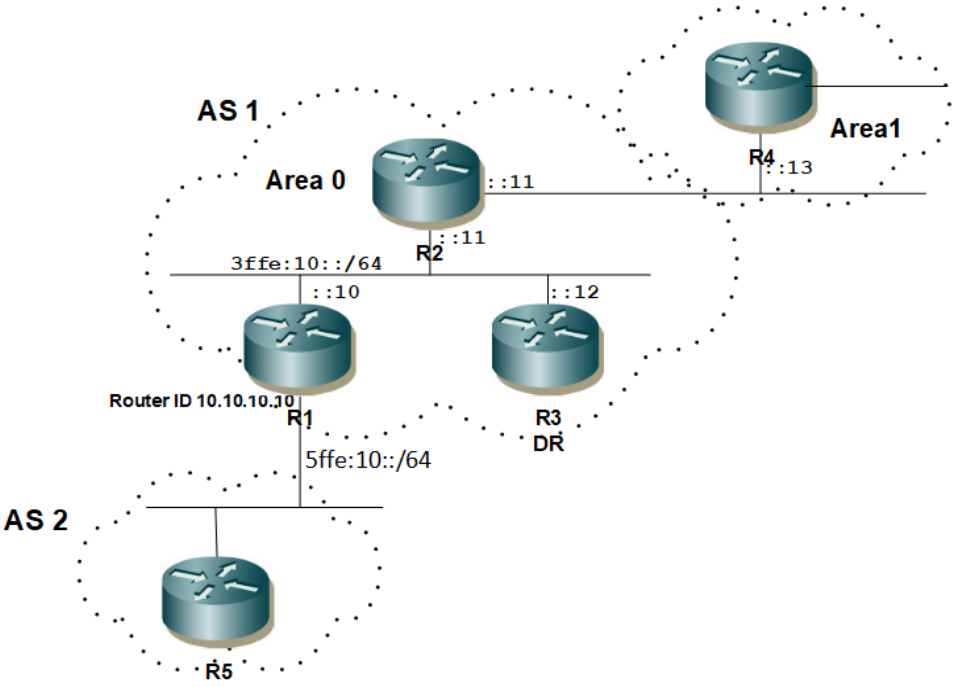


Figure 5-18: OSPFv3 Redistribute Routes

Configuration

R5

(config)#router bgp 2	Configure router bgp instance
(config-router)# neighbor 5ffe:10::10 remote-as 1	Configure R1 as ipv6 BGP neighbor
(config-router)# neighbor 5ffe:10::10 ebgp-multihop 4	Configure the ebgp -multihop for the ebgp neighbor R1
(config-router)# address-family ipv6 unicast	
(config-router-af)# neighbor 5ffe:10::10 activate	Activate the BGP neighbor on R1 for address-family ipv6 unicast to advertise and receive ipv6 routes

R1

#configure terminal	Enter configure mode.
(config)#router bgp 2	Configure router bgp instance
(config-router)# neighbor 5ffe:10::55 remote-as 2	Configure R5 as ipv6 BGP neighbor
(config-router)# neighbor 5ffe:10::55 ebgp-multihop 4	Configure the ebgp -multihop for the ebgp neighbor R5
(config-router)# address-family ipv6 unicast	
(config-router-af)# neighbor 5ffe:10::55 activate	Activate the BGP neighbor on R5 for address-family ipv6 unicast to advertise and receive ipv6 routes
(config-router-af)#exit	Exit address-family ipv6 unicast mode
(config-router)#exit	Exit router bgp mode
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.10.10	Specify a Router ID (10.10.10.10) for the OSPFv3 routing process.
(config-router)#redistribute bgp	Specify redistributing routes from the other routing protocol (BGP) into OSPFv3.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth12	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

Validation

R2

```
R2#show ipv6 ospf neighbor

Total number of full neighbors: 3
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.12       1   Full/Backup     00:00:31    eth1       0
10.10.10.10       1   Full/Backup     00:00:32    eth2       0
10.10.10.13      10   Full/DR         00:00:31    eth2       0
```

```
R2#

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.11     1327       0x80000006 0x9384      1
0.0.0.3         10.10.10.12     1180       0x80000006 0x1d21      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      348       0x80000008 0x8e91      1
0.0.0.4         10.10.10.11      300       0x80000008 0x33b6      1
0.0.0.4         10.10.10.13      387       0x80000009 0xcdee      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       24       0x8000000d 0xe6ad      1
0.0.0.0         10.10.10.11     1321       0x8000000b 0xe1b4      1
0.0.0.0         10.10.10.13      287       0x8000000b 0xd2c2      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13      287       0x80000009 0x98b7

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11     1321       0x80000006 0xd2a4

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13      287       0x80000009 0xcb47      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      284       0x8000000a 0x42ff
0.0.0.4         10.10.10.11      281       0x8000000a 0x6ed1
0.0.0.4         10.10.10.13      287       0x8000000a 0xc675

                Router-LSA (Area 0.0.0.1)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.11     1165       0x80000008 0x9b02      1
0.0.0.0         10.10.10.12     1162       0x80000008 0x920b      1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.11     1165       0x80000006 0x0c77

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11     1320       0x80000007 0xc2b4

                Inter-Area-Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11       25       0x80000005 0x941a

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.11     1165       0x80000006 0xcd4c      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.11     1165       0x80000007 0x66df
0.0.0.3         10.10.10.12     1162       0x80000007 0xf64b

                AS-external-LSA

Link State ID   ADV Router      Age       Seq#       CkSum   Route  Tag
0.0.0.1         10.10.10.10       65       0x80000002 0x284a E2      0

R2#

R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10        E   1          10.10.10.10          eth2
10.10.10.11         B  --
10.10.10.13            1          10.10.10.13          eth2

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.11         B  --
10.10.10.12            1          10.10.10.12          eth1
```

```
R2#

R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 2000::/64                                        1/20
     via fe80::5054:ff:fe2b:20b7, eth2
C  3ffe:10::/64                                      1
     directly connected, eth2, Area 0.0.0.0
C  3ffe:11::/64                                      1
     directly connected, eth1, Area 0.0.0.1
R2#

R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 03:49:59
O E2   2000::/64 [110/20] via fe80::5054:ff:fe2b:20b7, eth2, 00:36:38
C      3ffe:10::/64 via ::, eth2, 03:46:32
C      3ffe:11::/64 via ::, eth1, 03:01:21
C      fe80::/64 via ::, eth9, 03:49:59
R2#
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 2000::/64                                        1/20
     via fe80::5054:ff:fe2b:20b7, eth2
C  3ffe:10::/64                                      1
     directly connected, eth2, Area 0.0.0.0
```

```
IA 3ffe:11::/64                                          2
     via fe80::5054:ff:fe3d:e317, eth2, Area 0.0.0.0
R3#

R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 03:51:07
O E2   2000::/64 [110/20] via fe80::5054:ff:fe2b:20b7, eth2, 00:37:50
C      3ffe:10::/64 via ::, eth2, 03:47:35
O IA   3ffe:11::/64 [110/2] via fe80::5054:ff:fe3d:e317, eth2, 02:58:53
C      fe80::/64 via ::, eth9, 03:51:07
R3#
```

R4

R4#show ipv6 ospf route

OSPFv3 Process (*null*)

Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

Destination Metric

Next-hop

E2 2000::/64 2/20

via fe80::5054:ff:fe0e:46b7, eth1

IA 3ffe:10::/64 2

via fe80::5054:ff:fe0e:46b7, eth1, Area 0.0.0.1

C 3ffe:11::/64 1

directly connected, eth1, Area 0.0.0.1

R4#

```
R4#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime
```

```
IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 03:15:06
O E2    2000::/64 [110/20] via fe80::5054:ff:fe0e:46b7, eth1, 00:39:34
O IA    3ffe:10::/64 [110/2] via fe80::5054:ff:fe0e:46b7, eth1, 02:57:53
C       3ffe:11::/64 via ::, eth1, 03:04:04
C       fe80::/64 via ::, eth9, 03:15:06
R4#
```

Cost

Make a route the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 10. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+100 = 110

R3: 10+150 = 160

For this reason, R1 chooses R2 as its next hop to destination 10.10.14.0/24, because it has the lower cost.

Topology

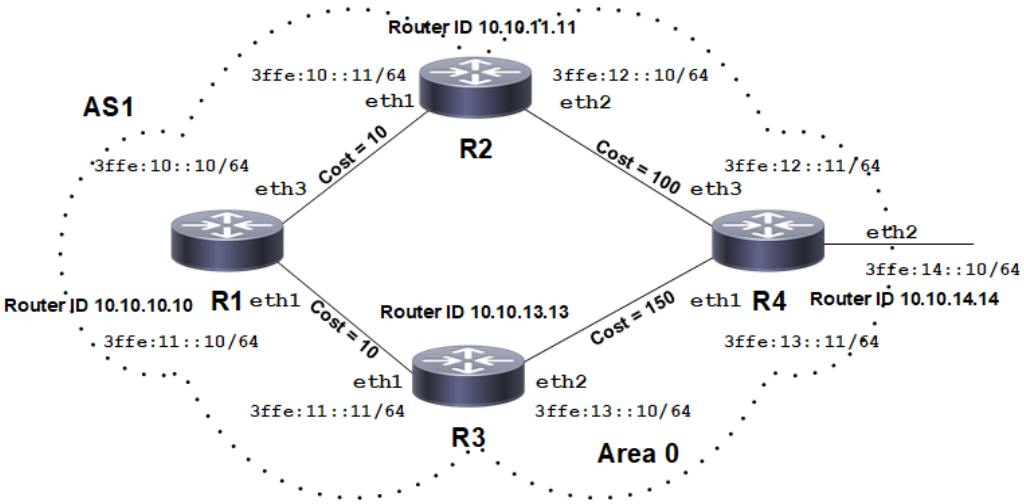


Figure 5-19: Configure Cost OSPFv3

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID (`10.10.10.10`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.

`#configure terminal`	Enter configure mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

R2

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.11.11`	Specify a Router ID (`10.10.11.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf cost 100`	Set the cost of the link-state metric (on `eth2`) to `100`.

R3

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.13.13`	Specify a Router ID (`10.10.13.13`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf cost 150`	Set the cost of link-state metric to `150`.

R4

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.14.14`	Specify a Router ID (`10.10.14.14`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID (`0`).

Validation

R1

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.13.13       1   Full/Backup     00:00:37    eth1       0
10.10.11.11       1   Full/Backup     00:00:34    eth3       0


R1#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
10.10.10.10           --
10.10.11.11           1          10.10.11.11         eth3
10.10.13.13           1          10.10.13.13         eth1
10.10.14.14           101        10.10.11.11         eth3



rtr1#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10      868       0x80000003 0x4839      1
0.0.0.3         10.10.13.13      747       0x80000003 0x5544      1

                Link-LSA (Interface eth3)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10      898       0x80000003 0xf33e      1
0.0.0.3         10.10.11.11      817       0x80000003 0xce7b      1
```

```
                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       58       0x80000008 0xabaf      2
0.0.0.0         10.10.11.11     1767       0x80000008 0x26cd      2
0.0.0.0         10.10.13.13     1753       0x80000008 0x9724      2
0.0.0.0         10.10.14.14     1753       0x80000007 0x96b5      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10       58       0x80000003 0x4341
0.0.0.5         10.10.10.10      163       0x80000003 0xf88d
0.0.0.4         10.10.11.11     1767       0x80000002 0x5c22
0.0.0.4         10.10.13.13     1753       0x80000002 0x680e

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10      813       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10      743       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11      652       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13      684       0x80000003 0x22ec      1  Network-
LSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10      868       0x80000004 0x4fe8
0.0.0.5         10.10.10.10      898       0x80000004 0x39fb
0.0.0.3         10.10.11.11      817       0x80000004 0x72c1
0.0.0.4         10.10.11.11      802       0x80000005 0xe1ea
0.0.0.3         10.10.13.13      747       0x80000004 0x5ad6
0.0.0.4         10.10.13.13      727       0x80000005 0x8f02
0.0.0.3         10.10.14.14      688       0x80000004 0x2df8
0.0.0.5         10.10.14.14      653       0x80000004 0x9c8c


rtr1#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
C  3ffe:10::/64                                        1
     directly connected, eth3, Area 0.0.0.0
C  3ffe:11::/64                                        1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                      101
     via fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0
O  3ffe:13::/64                                      102
     via fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0
```

```
rtr1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:22:59
C      3ffe:10::/64 via ::, eth3, 00:51:14
C      3ffe:11::/64 via ::, eth1, 00:50:44
O      3ffe:12::/64 [110/101] via fe80::a00:27ff:fef9:2432, eth3, 00:49:33
O      3ffe:13::/64 [110/102] via fe80::a00:27ff:fef9:2432, eth3, 00:48:21
C      fe80::/64 via ::, eth1, 01:13:13
K      ff00::/8 [0/256] via ::, eth0, 01:22:47
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:32    eth1       0
10.10.14.14       1   Full/Backup     00:00:33    eth2       0


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
10.10.10.10            1          10.10.10.10         eth1
10.10.11.11            --
10.10.13.13            2          10.10.10.10         eth1
10.10.14.14            100        10.10.14.14         eth2



R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.11.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10     1373       0x80000003 0xf33e      1
0.0.0.3         10.10.11.11     1290       0x80000003 0xce7b      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
```

```
0.0.0.4         10.10.11.11     1275       0x80000003 0x802a      1
0.0.0.5         10.10.14.14     1126       0x80000003 0x4f29      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      533       0x80000008 0xabaf      2
0.0.0.0         10.10.11.11      440       0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      427       0x80000009 0x9525      2
0.0.0.0         10.10.14.14      426       0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10      533       0x80000003 0x4341
0.0.0.5         10.10.10.10      638       0x80000003 0xf88d
0.0.0.4         10.10.11.11      440       0x80000003 0x5a23
0.0.0.4         10.10.13.13      427       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1288       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1218       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1125       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1158       0x80000003 0x22ec      1  Network-
LSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10     1343       0x80000004 0x4fe8
0.0.0.5         10.10.10.10     1373       0x80000004 0x39fb
0.0.0.3         10.10.11.11     1290       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1275       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1223       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1203       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1161       0x80000004 0x2df8
0.0.0.5         10.10.14.14     1126       0x80000004 0x9c8c


R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:10::/64                                      1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:11::/64                                      2
     via fe80::a00:27ff:fe6e:21d8, eth1, Area 0.0.0.0
C  3ffe:12::/64                                    100
     directly connected, eth2, Area 0.0.0.0
```

```
O  3ffe:13::/64                                    101
     via fe80::a00:27ff:fe01:c94d, eth2, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:26:25
C      3ffe:10::/64 via ::, eth1, 00:54:14
O      3ffe:11::/64 [110/2] via fe80::a00:27ff:fe6e:21d8, eth1, 00:55:03
C      3ffe:12::/64 via ::, eth2, 00:53:58
O      3ffe:13::/64 [110/101] via fe80::a00:27ff:fe01:c94d, eth2, 00:52:43
C      fe80::/64 via ::, eth2, 01:20:38
K      ff00::/8 [0/256] via ::, eth2, 01:20:39
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:33    eth1       0
10.10.14.14       1   Full/Backup     00:00:38    eth2       0



R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
10.10.10.10           1          10.10.10.10         eth1
10.10.11.11           2          10.10.10.10         eth1
10.10.13.13           --
10.10.14.14           102        10.10.10.10         eth1


R3#
R3#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.13.13) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10     1591       0x80000003 0x4839      1
0.0.0.3         10.10.13.13     1468       0x80000003 0x5544      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.13.13     1448       0x80000003 0x9d29      1
```

```
0.0.0.3         10.10.14.14     1409       0x80000003 0x50cf      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum    Link
0.0.0.0         10.10.10.10      780       0x80000008 0xabaf      2
0.0.0.0         10.10.11.11      689       0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      673       0x80000009 0x9525      2
0.0.0.0         10.10.14.14      673       0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10      780       0x80000003 0x4341
0.0.0.5         10.10.10.10      885       0x80000003 0xf88d
0.0.0.4         10.10.11.11      689       0x80000003 0x5a23
0.0.0.4         10.10.13.13      673       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1536       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1466       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1374       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1403       0x80000003 0x22ec      1  Network-
LSA
               Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10     1591       0x80000004 0x4fe8
0.0.0.5         10.10.10.10     1621       0x80000004 0x39fb
0.0.0.3         10.10.11.11     1539       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1524       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1468       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1448       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1409       0x80000004 0x2df8
0.0.0.5         10.10.14.14     1374       0x80000004 0x9c8c


R3#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  3ffe:10::/64                                     2
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0
C  3ffe:11::/64                                     1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                   102
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0
O  3ffe:13::/64                                   103
```

```
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0


R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:28:16
O      3ffe:10::/64 [110/2] via fe80::a00:27ff:fe7d:2a72, eth1, 00:58:14
C      3ffe:11::/64 via ::, eth1, 00:55:44
O      3ffe:12::/64 [110/102] via fe80::a00:27ff:fe7d:2a72, eth1, 00:56:36
C      3ffe:13::/64 via ::, eth2, 00:55:26
C      fe80::/64 via ::, eth1, 01:20:39
K      ff00::/8 [0/256] via ::, eth2, 01:21:40
```

R4

```
R4#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.13.13       1   Full/DR         00:00:30    eth1       0
10.10.11.11       1   Full/DR         00:00:30    eth3       0



R4#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
10.10.10.10            2          10.10.11.11         eth3
                                  10.10.13.13         eth1
10.10.11.11            1          10.10.11.11         eth3
10.10.13.13            1          10.10.13.13         eth1
10.10.14.14            --


R4#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.14.14) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.13.13     1634       0x80000003 0x9d29      1
0.0.0.3         10.10.14.14     1592       0x80000003 0x50cf      1

                Link-LSA (Interface eth3)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.11.11     1708       0x80000003 0x802a      1
```

```
0.0.0.5         10.10.14.14     1557       0x80000003 0x4f29      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum    Link
0.0.0.0         10.10.10.10      966       0x80000008 0xabaf      2
0.0.0.0         10.10.11.11      873       0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      859       0x80000009 0x9525      2
0.0.0.0         10.10.14.14      857       0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10      966       0x80000003 0x4341
0.0.0.5         10.10.10.10     1071       0x80000003 0xf88d
0.0.0.4         10.10.11.11      873       0x80000003 0x5a23
0.0.0.4         10.10.13.13      859       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1721       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1651       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1558       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1589       0x80000003 0x22ec      1  Network-
LSA

  Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10     1776       0x80000004 0x4fe8
0.0.0.5         10.10.10.10        6       0x80000005 0x37fc
0.0.0.3         10.10.11.11     1723       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1708       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1654       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1634       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1592       0x80000004 0x2df8
0.0.0.5         10.10.14.14     1557       0x80000004 0x9c8c



R4#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  3ffe:10::/64                                     2
     via fe80::a00:27ff:fe0d:fbe3, eth3, Area 0.0.0.0
O  3ffe:11::/64                                     2
     via fe80::a00:27ff:fecf:8873, eth1, Area 0.0.0.0
C  3ffe:12::/64                                     1
```

```
     directly connected, eth3, Area 0.0.0.0
C  3ffe:13::/64                                        1
     directly connected, eth1, Area 0.0.0.0


R4#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:32:01
O      3ffe:10::/64 [110/2] via fe80::a00:27ff:fe0d:fbe3, eth3, 01:02:49
O      3ffe:11::/64 [110/2] via fe80::a00:27ff:fecf:8873, eth1, 01:02:19
C      3ffe:12::/64 via ::, eth3, 00:58:46
C      3ffe:13::/64 via ::, eth1, 00:59:18
C      fe80::/64 via ::, eth1, 01:27:01
K      ff00::/8 [0/256] via ::, eth3, 01:27:31
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a non-contiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

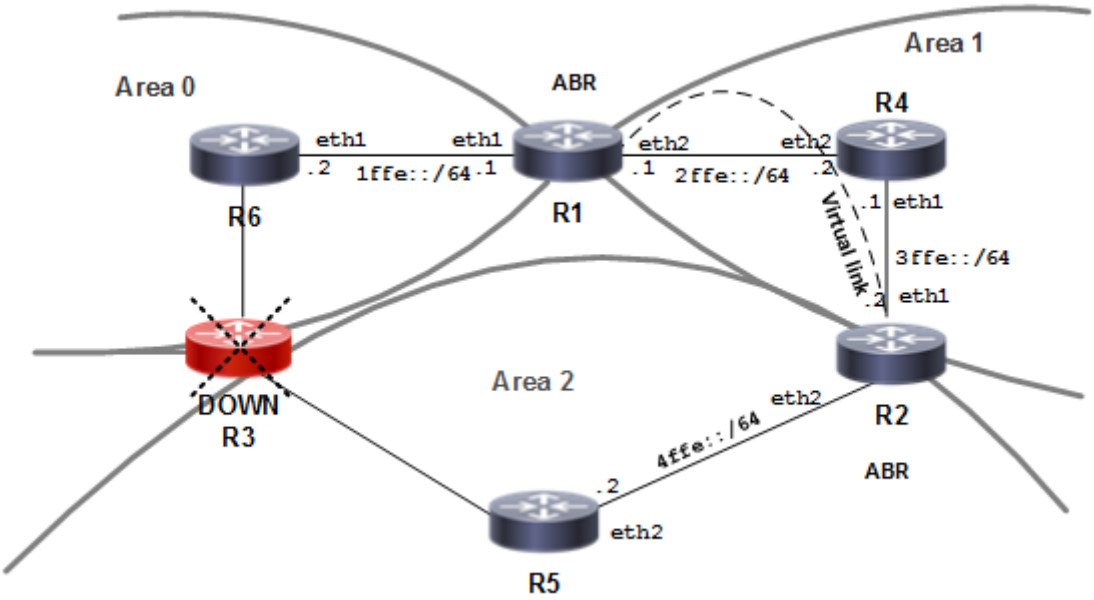


Figure 5-20: OSPFv3 Virtual Links

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Setup loopback interface
`(config-if)#ip address 1.1.1.1/32 secondary`	Specify loopback interface address
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on this interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on this interface, and assign the Area ID `(1)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#area 1 virtual-link 2.2.2.2`	Configure a virtual link between this router R1 and R2 (Router ID `2.2.2.2`) through transit area 1.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Setup loopback interface
`(config-if)#ip address 2.2.2.2/32 secondary`	Specify loopback interface address
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on this interface, and assign the Area ID `(1)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 2`	Enable OSPFv3 routing on this interface, and assign the Area ID `(2)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 2.2.2.2`	Specify a Router ID (`2.2.2.2`) for the OSPFv3 routing process.
`(config-router)#area 1 virtual-link 1.1.1.1`	Configure a virtual link between this router R1 and R2 (Router ID `1.1.1.1`) through transit area 1.

R4

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.

(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 4.4.4.4	Specify a Router ID (4.4.4.4) for the OSPFv3 routing process.

R5

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 2	Enable OSPFv3 routing on this interface, and assign the Area ID (2).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 5.5.5.5	Specify a Router ID (5.5.5.5) for the OSPFv3 routing process.

R6

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on this interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 6.6.6.6	Specify a Router ID (6.6.6.6) for the OSPFv3 routing process.

Validation

R2

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:31    eth1       0
3.3.3.3           1   Full/DR         00:00:32    eth2       0
2.2.2.2           1   Full/ -         inactive    VLINK2147479553 0


#show ipv6 ospf virtual-links
Virtual Link VLINK2147479553 to router 2.2.2.2 is up
```

```
  Transit area 0.0.0.1 via interface eth2, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 2ffe::11/128
  Remote address 3ffe::11/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 1.1.1.1
 Process uptime is 5 minutes
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 17
 Number of LSA received 50
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 2(2)
        SPF algorithm executed 8 times
        Number of LSA 23.  Checksum Sum 0xB35D8
        Number of Unknown LSA 0
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 13 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  1ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0
```

```
C  2ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
C  2ffe::11/128                                       0
     directly connected, eth2, TransitArea 0.0.0.1
O  3ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
O  3ffe::11/128                                       2
     via fe80::5054:ff:fe6f:334d, eth2, TransitArea 0.0.0.1
IA 4ffe::/64                                          3
     via fe80::5054:ff:fe6f:334d, eth2, TransitArea 0.0.0.1
#
```

R3

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:35    eth1       0
2.2.2.2           1   Full/Backup     00:00:30    eth2       0


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 3.3.3.3
 Process uptime is 5 minutes
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 10
 Number of LSA received 23
 Number of areas in this router is 1
    Area 0.0.0.1
        Number of interfaces in this area is 2(2)
        SPF algorithm executed 14 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
```

```
     Next-hop
IA 1ffe::/64                                          2
     via fe80::5054:ff:feb7:cc69, eth1, TransitArea 0.0.0.1
C  2ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
O  2ffe::11/128                                       1
     via fe80::5054:ff:feb7:cc69, eth1, TransitArea 0.0.0.1
C  3ffe::/64                                          1
     directly connected, eth1, TransitArea 0.0.0.1
O  3ffe::11/128                                       1
     via fe80::5054:ff:fec5:2430, eth2, TransitArea 0.0.0.1
IA 4ffe::/64                                          2
     via fe80::5054:ff:fec5:2430, eth2, TransitArea 0.0.0.1
```

R4

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
3.3.3.3           1   Full/DR         00:00:31    eth1       0
1.1.1.1           1   Full/ -         inactive    VLINK2147479554 0


#show ipv6 ospf virtual-links
Virtual Link VLINK2147479554 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface eth1, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 3ffe::11/128
  Remote address 2ffe::11/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 2.2.2.2
 Process uptime is 4 minutes
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 26
 Number of LSA received 37
```

```
 Number of areas in this router is 3
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 3 times
        Number of LSA 23.  Checksum Sum 0xB35D8
        Number of Unknown LSA 0
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 11 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
    Area 0.0.0.2
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 4 times
        Number of LSA 11.  Checksum Sum 0x5D8B7
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  1ffe::/64                                         3
     via fe80::5054:ff:fe1d:eace, eth1, TransitArea 0.0.0.1
O  2ffe::/64                                         1
     directly connected, eth1, TransitArea 0.0.0.1
O  2ffe::11/128                                      2
     via fe80::5054:ff:fe1d:eace, eth1, TransitArea 0.0.0.1
C  3ffe::/64                                         1
     directly connected, eth1, TransitArea 0.0.0.1
C  3ffe::11/128                                      0
     directly connected, eth1, TransitArea 0.0.0.1
C  4ffe::/64                                         1
     directly connected, eth2, Area 0.0.0.2
```

Multiple Instances

By using multiple OSPFv3 instances, OSPFv3 routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

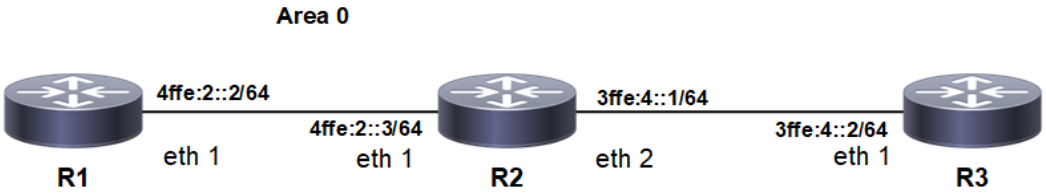
To configure multiple OSPFv3 instances, refer to the topology diagram and follow the procedures below.

1. Enable OSPFv3 on an interface.
2. Enable multiple instances.

3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type, or route-map options.

Topology



Enable Multiple OSPFv3 Instances on a Router Based on Tags

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPFv3.

R1

`(config)#router ipv6 ospf 5`	Configure an OSPFv3 instance with an instance ID of 5.
`(config-router)#router-id 5.5.5.5`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe:2::2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 5`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

R2

`(config)#router ipv6 ospf 5`	Configure an OSPFv3 instance with an instance ID of 5.
`(config-router)#router-id 149.149.149.149`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Configure the interface to connect to R1.
`(config-if)#ipv6 address 4ffe:2::3/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 5`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure terminal mode.
`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with an instance ID of 15.
`(config-router)#router-id 159.159.159.159`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth2`	Configure the interface to connect to R3.
`(config-if)#ipv6 address 3ffe:4::1/64`	Configure the IPv6 address.

(config-if)#no shutdown	Activate the interface.
(config-if)#ipv6 router ospf area 0 tag 15	Configure the area number and instance value: match the instance ID with the instance ID created previously.

R3

(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with an instance ID of 15.
(config-router)#router-id 152.152.152.152	Configure the router ID to use on this instance.
(config-router)#exit	Exit Router mode, and return to Interface mode.
(config)#interface eth1	Specify the interface on which OSPFv3 is to be enabled.
(config-if)#ipv6 address 3ffe:4::2/64	Configure the IPv6 address.
(config-if)#ipv6 router ospf area 0 tag 15	Configure the area number and instance value: match the instance ID with the instance ID created previously.
(config-if)#no shutdown	Activate the interface.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0

R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth2, Area 0.0.0.0

OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:35    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:33    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0


R3#sh ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:34    eth1       0
```

Redistribute among Multiple Instances

In this example, routes of one ospfv3 instance are redistributed to another ospfv3 instance to enable ping from R1 to R3 or vice-versa; and R2 redistributes routes from one instance to another.

R2

(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with instance ID 15.
(config-router)#router-id 159.159.159.159	Configure the router ID.
(config-router)#redistribute ospf 5	Redistribute instance 5 routes.
(config-router)#exit	Exit OSPF router mode.
(config)#router ipv6 ospf 5	Configure an OSPFv3 instance with instance ID 5.
(config-router)#router-id 149.149.149.149	Configure the router ID.
(config-router)#redistribute ospf 15	Redistribute instance 15 routes.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:34    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:30    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
```

```
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20
     via fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:33    eth1       0
```

Redistribute with Metric Option

In this example, on R3, routes of instance 15 are redistributed into instance and vice-versa with metric of 100 so that R1 and R2 have each other's routes with a metric of 100.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID 15.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 metric 100`	Redistribute instance 5 routes with metric 100.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance 5.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 metric 100`	Redistribute instance 15 routes with metric 100.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
E2 3ffe:4::/64                                        1/100
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                           1
     directly connected, eth1, Area 0.0.0.0
R1#

R1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
```

```
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 18:08:02
O E2   3ffe:4::/64 [110/100] via fe80::5054:ff:fe0e:46b7, eth1, 00:00:25
C      4ffe:2::/64 via ::, eth1, 00:20:39
C      fe80::/64 via ::, eth9, 18:08:02
R1#


R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:36    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0



R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:33    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:40    eth1       0
```

R3

```
R3#show ipv6 ospf route
```

```
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/100
     via fe80::a00:27ff:fe0d:fbe3, eth1

R3#

R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 18:08:13
C      3ffe:4::/64 via ::, eth1, 00:17:55
O E2   4ffe:2::/64 [110/100] via fe80::5054:ff:fe3d:e317, eth1, 00:01:05
C      fe80::/64 via ::, eth9, 18:08:13
R3#


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:37    eth1       0
```

Redistribute with Type Option

In this example, on R3, R1 has R3 routes as type 2, and R3 has R1 routes as type 1.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID 15.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 metric-type 1`	Redistribute instance 5 routes as type 1.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance 5.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 metric-type 2`	Redistribute instance 15 routes as type 2.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
152.152.152.152   1   Full/DR         00:00:36    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
5.5.5.5           1   Full/DR         00:00:32    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/21
     via fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
159.159.159.159   1   Full/Backup     00:00:36    eth1       0
```

Redistribute with Route-Map Option

R1

`(config)#interface eth2`	Configure the interface eth2 on R1.
`(config-if)#ipv6 address 4ffe:1::2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 5`	Configure interface eth2 for ospfv3 with area 0 and instance 5

Validation

```
R3
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth1, Area 0.0.0.0
E1 4ffe:1::/64                                        20
     via fe80::5054:ff:fe3d:e317, eth1
E1 4ffe:2::/64                                        20
     via fe80::5054:ff:fe3d:e317, eth1
R3#
```

R2

`R2(config)#ipv6 prefix-list permit-4ffe-2 permit 4ffe:2::/64`	Configure and ipv6 prefix-list to permit the prefix 4ffe:2::/64
`R2(config)#route-map permit-only-4ffe-2`	Configure a route-map to permit only the prefix 4ffe:2::/64

`R2(config-route-map)#match ipv6 address prefix-list permit-4ffe-2`	Configure a match statement to match the configured ipv6 prefix-list
`R2(config-route-map)#exit`	Exit route-map mode and return to configure terminal mode
`R2(config)#router ipv6 ospf 15`	Enter router ipv6 mode for instance 15
`R2(config-router)#redistribute ospf 5 route-map permit-only-4ffe-2`	Redistribute instance 5 routes with route-map to permit only the ipv6 prefix 4ffe:2::/64
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance 5.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 route-map 1`	Redistribute instance 15 routes with route map 1.
`(config-router)#redistribute connected`	Redistribute connected routes to instance 15.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::5054:ff:fe0e:46b7, eth1
C  4ffe:1::/64                                         1
     directly connected, eth2, Area 0.0.0.0
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0
R1#

R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
149.149.149.149   1   Full/DR         00:00:34    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  4ffe:1::/64                                        2
     via fe80::5054:ff:fe0c:40ed, eth1, Area 0.0.0.0
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0
R2#


R2#sh ipv6  ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/Backup     00:00:32    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/Backup     00:00:38    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20
     via fe80::5054:ff:fe3d:e317, eth1
R3#
```

Not-So-Stubby Area

This section contains OSPFv3 NSSA (Not-So-Stubby Area) configuration examples.

An NSSA allows external routes to be advertised into the OSPF autonomous system while retaining the characteristics of a stub area to the rest of the autonomous system. To do this, the ASBR in an NSSA will originate type 7 LSAs to advertise the external destinations. These NSSA external LSAs are flooded throughout the NSSA but are blocked at the ABR.

The NSSA external LSA has a flag in its header known as the P-bit. The NSSA ASBR has the option of setting or clearing the P-bit. If an NSSA's ABR receives a type 7 LSA with the P-bit set to one, it translates the type 7 LSA into a type 5 LSA and floods it throughout the other areas. If the P-bit is set to zero, no translation takes place and the destination in the type 7 LSA is not advertised outside of the NSSA.

Topology

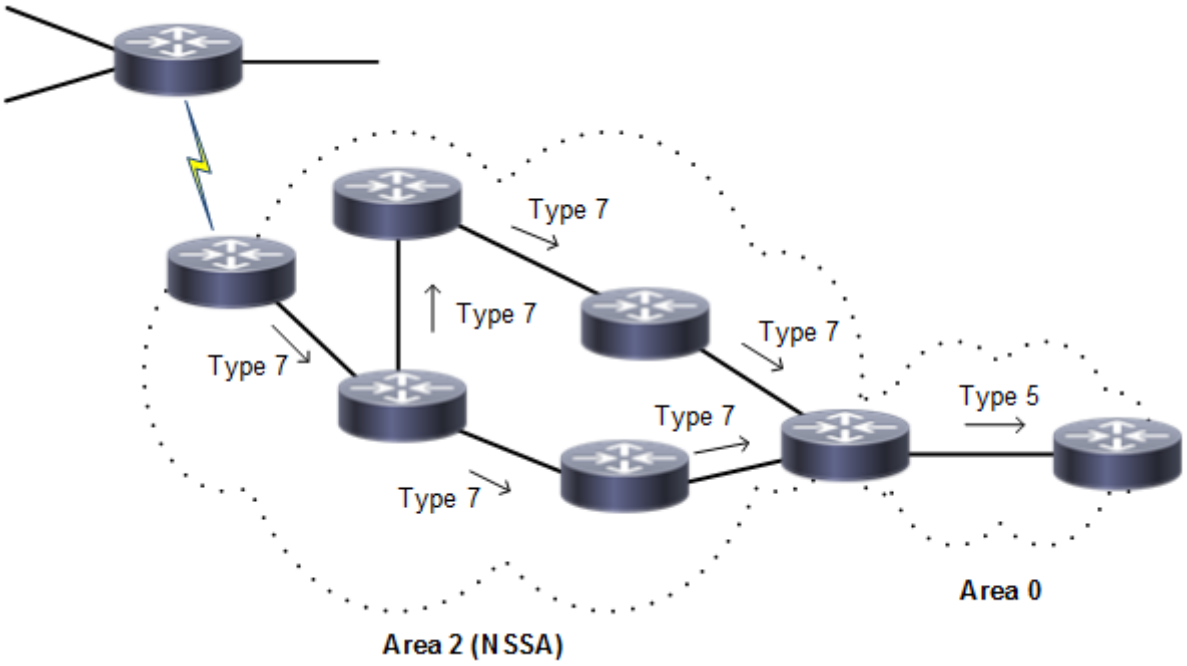


Figure 5-21: Translating Type 7 LSAs into Type 5 LSAs

NSSA with Route Option

This example shows the configuration to enable NSSA and to configure different route options for NSSA. There are three `area nssa` command options for originating default Type-3 LSA and default Type-7 LSA, and for blocking redistribution of Type-7 LSA into an NSSA:

- `no-summary`: The NSSA ABR blocks all type-3 and type-4 LSAs into the NSSA area and sends a single type-3 LSA into the area to advertise a default route
- `default-information-originate`: The NSSA ABR advertises a default route into the NSSA as a type-7 LSA.
- `no-redistribution`: The NSSA ABR bocks type-7 LSA from being redistributed into the NSSA area.

In Figure 5-22, R2 is an NSSA ABR as well as an NSSA ASBR that maps the router interfaces to two different areas and redistributes the connected routes of the loopback interface. Also, this example sets the `no-summary`, `no-redistribution`, and `default-information-originate` options on R2 to originate default Type-3 LSAs and default Type-7 LSAs into the NSSA and to block Type-7 LSAs.

Topology

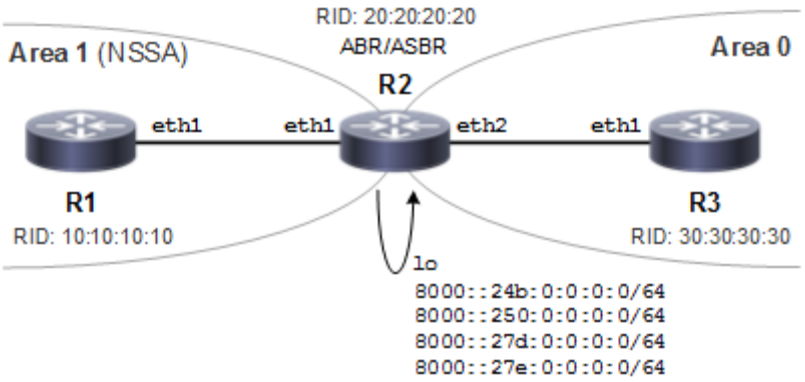


Figure 5-22: NSSA with Route Options

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure area as NSSA
`(config-router)#exit`	Exit interface mode

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone
`(config-if)#interface lo`	Enter interface mode for Loopback
`(config-if)#ipv6 address 8000::24b:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::250:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27d:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27e:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance (100)
`(config-router)#redistribute connected`	Redistribute the configured loopback network into the NSSA

`(config-router)#area 1 nssa no-redistribution default-information-originate no-summary`	Configure the Router to originate default Type-3 LSAs and default Type-7 LSAs, and to block Type-7 LSAs into the NSSA
`(config-router)#exit`	Exit interface mode

R3

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 30.30.30.30`	Configure the router ID to use on this instance (100)
`(config-router)#exit`	Exit interface mode

Validation 1

In the output of `show ipv6 ospf neighbor` below, verify that OSPFv3 adjacency is in state “full” for both R1 and R2 under the process identifier 100.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/DR         00:00:34    eth1       0

R2#show ipv6 ospf neighbor

Total number of full neighbors: 2
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:36    eth1       0
30.30.30.30       1   Full/Backup     00:00:39    eth2       0
R2#
```

Validation 2

The output below shows originating default Type-3 LSAs into the NSSA with the no-summary option. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and the LS-Type is Inter-Area-Prefix-LSA for the default Type-3 LSA route into the NSSA.

```
R1#sh ipv6 ospf database inter-prefix

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

  LS age: 1234
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.6
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000001
  Checksum: 0x17D0
  Length: 28
```

```
        Metric: 1
        Prefix: ::/0
        Prefix Options: 0
```

Validation 3

The output below shows originating default type-7 LSAs alone after setting the no-redistribution and default-information originate options. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and LS-Type is NSSA-external-LSA for the default Type-7 LSA route into the NSSA

```
    R1#sh ipv6 ospf database nssa-external

                OSPFv3 Router with ID (10.10.10.10) (Process 100)

                    NSSA-external-LSA (Area 0.0.0.1)

      LS age: 1758
      LS Type: NSSA-external-LSA
      Link State ID: 0.0.0.20
      Advertising Router: 20.20.20.20
      LS Seq Number: 0x80000002
      Checksum: 0x6468
      Length: 32
        Metric Type: 2 (Larger than any link state path)
        Metric: 1
        Prefix: ::/0
        Prefix Options: 0 (-|-|-|-)
        External Route Tag: 0
```

NSSA with the Summary Address Option

Figure 5-23 shows the configuration to originate external LSAs (Type-7) and translate them into external LSAs (Type-5):

- R1 is an NSSA-ASBR configured with loopback IPv6 addresses that are redistributed into OSPFv3
- R2 is an NSSA-ABR
- R3 is backbone router

R1 originates Type-7 LSAs which are summarized into a single Type-7 into the NSSA by the `summary-address` option and this summarized Type-7 is converted to Type-5 LSA by R2.

Also, the summarized route can be tagged using the `tag` command and the advertisement of summarized routes can be suppressed by the `not-advertise` option.

Topology

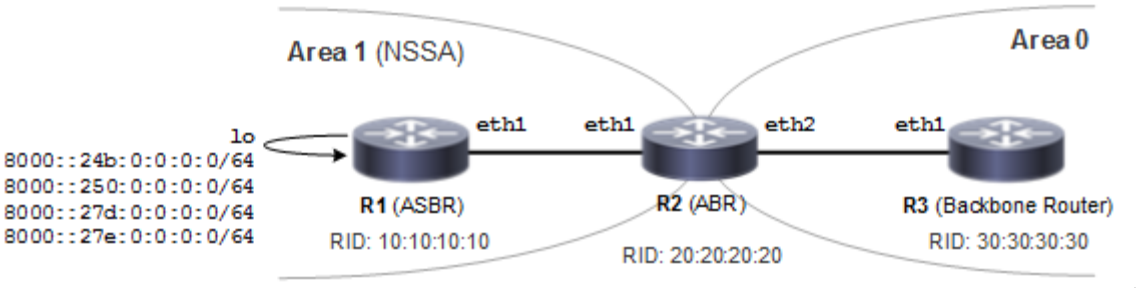


Figure 5-23: Using the summary-address Option

Configuration

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 address 1000::1/64`	Configure ipv6 address for interface eth1
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config-if)#interface lo`	Enter interface mode for loopback
`(config-if)#ipv6 address 8000::24b:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::250:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27d:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27e:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure the area as NSSA.
`(config-router)#redistribute connected`	Redistribute the configured loopback network into OSPFv3 NSSA. Note: Connected networks can be redistributed by setting the metric and metric type.
`(config-router)#summary-address 8000::/48 all-tag 10`	Summarize the address range and tag the summarized route
`(config-router)#exit`	Exit interface mode

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 address 1000::2/64`	Configure ipv6 address for interface eth1
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).

(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2
(config-if)#ipv6 address 2000::1/64	Configure ipv6 address for interface eth2
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 20.20.20.20	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa	Configure the Router in NSSA
(config-router)#exit	Exit interface mode

R3

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 address 2000::2/64	Configure ipv6 address for interface eth1
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 30.30.30.30	Configure the router ID to use on this instance (100)
(config-router)#exit	Exit interface mode

In the configurations above, you can suppress the external route summarization by NSSA-ASBR by specifying the not-advertise parameter as shown below:

```
(config-router)#summary-address 8000::/48 not-advertise
```

Also, connected networks can be redistributed by setting the metric and metric type as shown below:

```
(config-router)#redistribute connected metric 20 metric-type 1
```

Validation 1

The output below shows the summarized route generated by NSSA-ASBR (R1) with a tag. The output has the LS Type as NSSA-external-LSA with advertising router identifier (10.10.10.10) of the NSSA-ASBR (R1). Also, check the Prefix which is summarized route and external route tag as configured.

```
R1#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 90
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.11
  Advertising Router: 10.10.10.10
  LS Seq Number: 0x80000003
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 8 (P|-|-|-)
```

```
    External Route Tag: 10
```

Validation 2

```
The output below on the NSSA-ABR that is translating Type-7 LSAs to Type-5
LSAs shows summarized address in Type-7 and Type-5 LSA. Check for the same
prefix, external route tag in both Type7 and Type-5 LSA.
R2#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 241
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.11
  Advertising Router: 10.10.10.10
  LS Seq Number: 0x80000003
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 8 (P|-|-|-)
    External Route Tag: 10

R2#sh ipv6 ospf database external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                AS-external-LSA

  LS age: 245
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000003
  Checksum: 0x8660
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 10
```

Validation 3

The output below on the backbone router shows the summarized address in the translated Type-5 LSA. The prefix and external route tag are the same as the summarized Type-7 LSA originated by R1.

```
R3#sh ipv6 ospf database external

            OSPFv3 Router with ID (30.30.30.30) (Process 100)

                AS-external-LSA
```

```
LS age: 409
LS Type: AS-External-LSA
Link State ID: 0.0.0.3
Advertising Router: 20.20.20.20
LS Seq Number: 0x80000003
Checksum: 0x8660
Length: 40
  Metric Type: 2 (Larger than any link state path)
  Metric: 21
  Prefix: 8000::/48
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 10
```

NSSA with the Translator Role Option

Type-7 to Type-5 translation is done by an NSSA-ABR. If an NSSA has multiple NSSA-ABRs, only one will perform the translation. The NSSA-ABR translator role options are:

- Candidate (default)
- Always

In the topology in Figure 5-24:

- R1 is NSSA-ASBR
- R2 and R3 are NSSA-ABRs
- R4 is a backbone router

In this example, the NSSA translator role `candidate` is configured on both NSSA-ABRs (R2 and R3). The Type-7 to Type-5 translation is done by the router with the higher router identifier (R3).

Topology

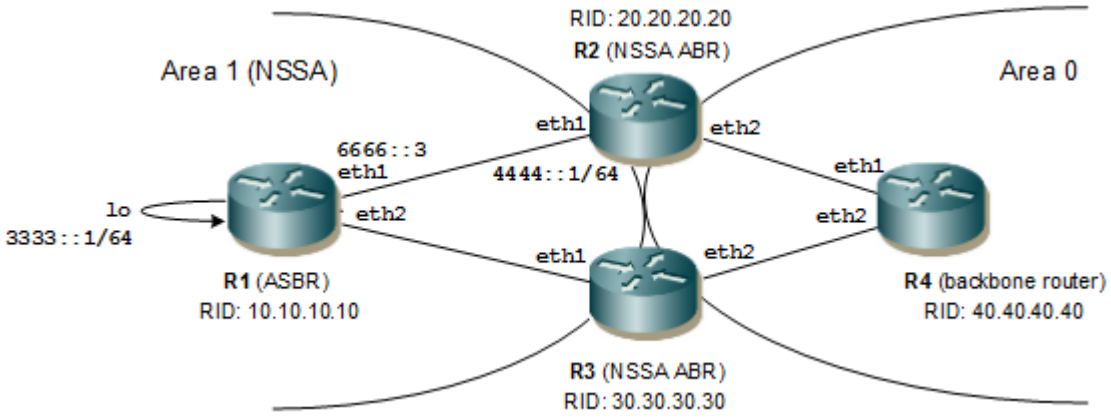


Figure 5-24: Using the translator-role Option

Configuration

When one NSSA-ABR is configured with the translator role as `always` and the other as `candidate`, then translation is done by the router configured as `always`. In this scenario, the translation can be biased by setting the translator role to `always` on the router that has the lower router identifier.

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config-if)#interface lo`	Enter interface mode for Loopback
`(config-if)#ipv6 address 3333::1/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure the area as NSSA.
`(config-router)#redistribute static`	Redistribute the static route configured into the OSPF NSSA
`(config-router)#redistribute connected`	Redistribute the connected network into OSPF NSSA
`(config-router)#exit`	Exit interface mode
`(config)#ipv6 route 4444::1/64 6666::3`	Configure the static route with the nexthop address as R2's `eth1` IPv6 address
`(config)#exit`	Exit interface mode.

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa translator-role candidate`	Configure the NSSA-ABR with the translator role candidate.
`(config-router)#exit`	Exit interface mode

R3

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.

`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 30.30.30.30`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa translator-role candidate`	Configure the NSSA-ABR with the translator role candidate.
`(config-router)#exit`	Exit interface mode

R4

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 40.40.40.40`	Configure the router ID to use on this instance (100)
`(config-router)#exit`	Exit interface mode

The command to configure the NSSA-Translator role as `always` is:

```
(config-router)#area 1 nssa translator-role always
```

The NSSA-ABR can continue to perform translation after its services are no longer required for the stability interval which is set using the command below on the NSSA-ABR.

```
(config-router)#area 1 nssa stability-interval 7777
```

Validation 1

The translation is done by the NSSA-ABR with the higher router identifier. In the output below, check the router identifier of the NSSA-ABR. Also, check the router which is elected and the router which is disabled.

```
R2#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID 20.20.20.20
 Process uptime is 21 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum Sum 0x1F816
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 28
 Number of LSA received 58
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 7 times
        Number of LSA 19.  Checksum Sum 0x7454D
        Number of Unknown LSA 0
    Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 14 times
        Number of LSA 19.  Checksum Sum 0xA4D18
        Number of Unknown LSA 0
```

```
        NSSA Translator State is disabled
R3#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID 30.30.30.30
 Process uptime is 19 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum Sum 0x1F816
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 31
 Number of LSA received 69
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 15 times
        Number of LSA 19.  Checksum Sum 0x7454D
        Number of Unknown LSA 0
    Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 10 times
        Number of LSA 19.  Checksum Sum 0xA4D18
        Number of Unknown LSA 0
        NSSA Translator State is elected
```

Validation 2

The translated Type-5 LSA in R4 in area 0 has the advertising router identifier of R3. In the output below, the LS Type is AS-External-LSA and the advertising router has the higher router identifier.

```
R4#sh ipv6 ospf database external

            OSPFv3 Router with ID (40.40.40.40) (Process 100)

                AS-external-LSA

  LS age: 885
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.7
  Advertising Router: 30.30.30.30
  LS Seq Number: 0x80000001
  Checksum: 0xD3FE
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 3333::/64
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0


  LS age: 18
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.8
  Advertising Router: 30.30.30.30
  LS Seq Number: 0x80000003
  Checksum: 0x7457
```

```
Length: 56
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 4444::/64
  Prefix Options: 0 (-|-|-|-)
  Forwarding Address: 6666::3
  External Route Tag: 0
```

Link LSA Suppression

If link LSA suppression is enabled and the interface type is not broadcast or NBMA, the router will not originate a link-LSA for the link. This implies that other routers on that link will determine the router's next hop address using a mechanism other than the link LSA.

Topology

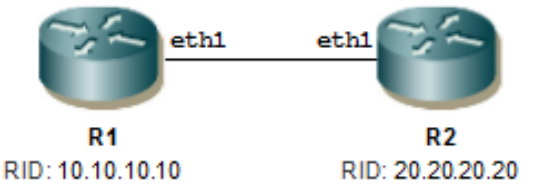


Figure 5-25: LSA Suppression

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf tag 100-ABC area 1`	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
`(config-if)#ipv6 ospf network point-to-point`	Configure the OSPF interface network type as point to point
`(config-if)#ipv6 ospf link-lsa-suppression enable`	Enable the link LSA suppression mechanism
`(config-if)#exit`	Exit interface mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance.

(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf tag 100-ABC area 1	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
(config-if)#ipv6 ospf network point-to-point	Configure the OSPF interface network type as point to point
(config-if)#ipv6 ospf link-lsa-suppression enable	Enable the link LSA Suppression Mechanism
(config-if)#exit	Exit interface mode

Note: This is not applicable for broadcast and NBMA networks.

Validation 1

Verify that adjacency has been established.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/ -         00:00:37    eth2       0
```

Validation 2

Verify that R1 should not have the Link LSA in the Link state database.

Note: The output below is captured after link lsa suppression enabled which has not Link LSA in the LSDB.

```
R1#sh ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process 100-ABC)

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         10.10.10.10       15 0x80000004 0x3264      1
0.0.0.0         20.20.20.20       15 0x80000002 0xdbba      1

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.12        10.10.10.10       14 0x80000004 0xaab4      1  Router-LSA
0.0.0.13        20.20.20.20       15 0x80000002 0x8f7f      1  Router-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.4         10.10.10.10       15 0x80000004 0xa326
0.0.0.3         20.20.20.20       15 0x80000002 0xffec
R1#sh ipv6 ospf database link

            OSPFv3 Router with ID (10.10.10.10) (Process 100-ABC)
```

Address Family IPv4 Unicast Configuration

This chapter contains basic OSPFv3 address family IPv4 unicast configuration examples.

The address family feature lets OSPFv3 IPv6 networks support both IPv6 and IPv4 unicast traffic. It uses multiple instance identifiers to support multiple address families. By default OSPFv3 supports only IPv6 unicast traffic.

The purpose of supporting address families in OSPFv3 is to advertise IPv4 unicast address family routes in OSPFv3 by assigning different instance identifier ranges to different address families. With this feature, users may have two router processes per interface, but only one process per address family. Each instance identifier implies a separate OSPFv3 instance with its own neighbor adjacencies, link state database, and SPF computation. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the same interface is not supported.

Enable Address Family IPv4 Unicast

The diagram below shows the minimum configuration required to enable the OSPFv3 address family feature and to establish the adjacency between R1 and R2 to support the IPv4 address family.

Note: To enable the IPv4 unicast address family in an OSPFv3 router, you need to configure an IPv4 address on the OSPFv3 enabled interface.

Topology

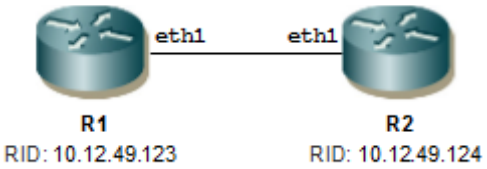


Figure 5-26: IPv4 Address Family on OSPFv3

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 11.1.1.1/24`	Assign IPv4 address to interface eth1
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use for this process .
`(config-router)#address-family ipv4 unicast`	Enable the ipv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode

(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in area 0. The tag uniquely identifies the routing process and the instance identifier is 64-95 for the IPv4 address family
(config-if)#exit	Exit interface mode

R2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 11.1.1.2/24	Assign IPv4 address to interface eth1
(config-if)#exit	Exit interface mode
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.124	Configure the router ID to use on this tag.
(config-router)#address-family ipv4 unicast	Enable the ipv4 address family
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in area 0. The tag uniquely identifies the routing process and the instance identifier is 64-95 for the IPv4 address family
(config-if)#end	Exit interface mode

Note: Use the process identifier to tag the interface, The instance identifier should be same on R1 and R2. In the above example, the process identifiers (100-ABC) and the instance identifiers are the same (64).

Validation

Verify that adjacency has been established with the configured instance identifier.

```
R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.12.49.123      1   Full/DR         00:00:37    eth1           64

R2#sh ipv6 ospf interface eth1
eth1 is up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::5054:ff:fe4e:32d1/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 64
    Router ID 10.12.49.124, Network Type BROADCAST, Cost: 1, TE Metric: 0
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 10.12.49.123
      Interface Address fe80::5054:ff:fe7e:3466
    Backup Designated Router (ID) 10.12.49.129
      Interface Address fe80::5054:ff:fe4e:32d1
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:04
    Neighbor Count is 1, Adjacent neighbor count is 1
```

Originate Type-7 LSAs and Translate to Type-5

Figure 5-27 shows the configuration to originate Type-7 LSAs and translate them into Type-5 LSAs. R3 is an NSSA-ASBR that originates Type-7 LSAs into the NSSA which are converted to Type-5 LSAs by R2 which is an NSSA-ABR. R1 is a backbone router.

Topology

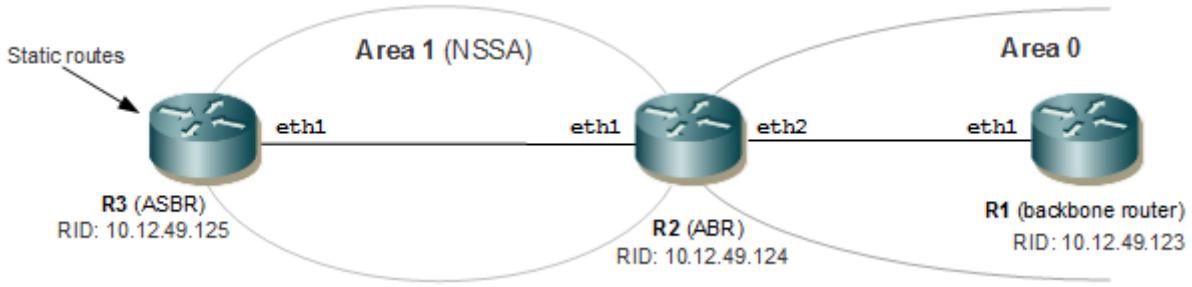


Figure 5-27: Originate Type-7 LSAs and Translate to Type-5 under Address Family IPv4

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 11.1.1.1/24`	Assign IPv4 address to interface eth1
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use on this tag
`(config-router)#address-family ipv4 unicast`	Enable the IPv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 11.1.1.2/24`	Assign IPv4 address to interface eth1
`(config-if)#exit`	Exit interface mode

(config)#interface eth2	Enter interface mode
(config-if)#ip address 22.1.1.1/24	Assign IPv4 address to interface eth2
(config-if)#exit	Exit interface mode
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.124	Configure the router ID to use for this process
(config-router)#area 1 nssa	Configure the area 1 as NSSA.
(config-router)#address-family ipv4 unicast	Enable the ipv4 address family
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode

R3

#configure terminal	Enter configure mode.
(config-router)#ip route 15.15.15.0/24 null	Configure the static route with the nexthop address set to null
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process
(config-router)#area 1 nssa	Configure the area 1 as NSSA.
(config-router)#address-family ipv4 unicast	Enable the ipv4 address family
(config-router-af)#redistribute static	Redistribute the static routes configured into the OSPF NSSA
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

Validation 1

Verify that adjacency has been established with the configured instance identifier.

```
R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface   Instance ID
```

```
10.12.49.123      1   Full/DR         00:00:31       eth1           64
10.12.49.125      1   Full/Backup     00:00:38    eth2          65
```

Validation 2

Verify that R3 has generated a Type-7 LSA and that the ABR R2 has External LSA Type 5 in its Database.

R3

```
R3#show ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.12.49.125) (Process 100-ABC)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 139
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.125
  LS Seq Number: 0x80000001
  Checksum: 0xAB34
  Length: 48
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 15.15.15.0/24
    Prefix Options: 8 (P|-|-|-)
    Forwarding Address: 22.1.1.2
    External Route Tag: 0


R3#show ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.125) (Process 100-ABC)

R3#
```

Validation 3

R2

```
R2#show ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.12.49.124) (Process 100-ABC)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 105
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.125
  LS Seq Number: 0x80000001
  Checksum: 0xAB34
```

```
  Length: 48
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 15.15.15.0/24
    Prefix Options: 8 (P|-|-|-)
    Forwarding Address: 22.1.1.2
    External Route Tag: 0

R2#

R2#show ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.124) (Process 100-ABC)

                AS-external-LSA

  LS age: 706
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.124
  LS Seq Number: 0x80000001
  Checksum: 0xAB1F
  Length: 48
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 15.15.15.0/24
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 22.1.1.2


R2#

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.0.0.0/8 is directly connected, eth0, 15:43:05
C            11.1.1.0/24 is directly connected, eth1, 14:54:49
O N2         15.15.15.0/24 [110/20] via 22.1.1.2, eth2, 12:09:25
C            22.1.1.0/24 is directly connected, eth2, 12:22:45
C            127.0.0.0/8 is directly connected, lo, 15:43:05

Gateway of last resort is not set
R2#
```

Validation 3

Verify that FIB of backbone router has External Route as “O E2”.

```
R1#
```

```
Verify that FIB of backbone router R1 has External Route as "O E2".
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.0.0.0/8 is directly connected, eth0, 03:34:25
C            11.1.1.0/24 is directly connected, eth1, 02:46:18
O E2         15.15.15.0/24 [110/20] via 11.1.1.2, eth1, 00:00:36
O IA         22.1.1.0/24 [110/2] via 11.1.1.2, eth1, 00:05:01
C            127.0.0.0/8 is directly connected, lo, 03:34:25

Gateway of last resort is not set
```

Summarize Inter-Area and External Routes

Figure 5-28 shows the configuration to enable inter-area and external route summarization. The IPv4 address family is enabled on R1. R2 summarizes the internal OSPF routes which R3 redistributes.

Topology

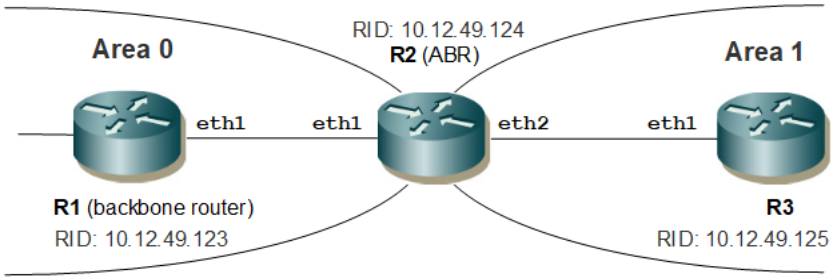


Figure 5-28: Enabling Intra-Area and External Route Summarization

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use for this process.
`(config-router)#address-family ipv4 unicast`	Enable the IPv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode

(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.10.10.1/24	Specify IP address for interface eth1
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

R2

(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.10.10.2/24	Specify an IP address for the interface
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.20.20.1/24	Specify an IP address for the interface
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode
(config)#interface lo	Enter interface mode
(config-if)# ip address 100.1.1.100/32 secondary	Specify an IP address for the interface
(config-if)# ip address 100.1.1.110/32 secondary	Specify an IP address for the interface
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode
#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process
(config-router)#router-id 10.12.49.124	Configure the router ID to use for this process
(config-router)#address-family ipv4 unicast	Enable the IPv4 address family
R2(config-router-af)#area 1 range 100.1.1.0/24 advertise	Summarize the inter-area OSPF routes
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode

R3

(config)#interface eth1	Enter interface mode
(config-if)#ip address 20.20.20.2/24	Specify an IP address for the interface
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

(config)#interface lo	Enter interface mode
(config-if)# ip address 200.1.1.100/32 secondary	Specify an IP address for the interface
(config-if)# ip address 200.1.1.110/32 secondary	Specify an IP address for the interface
(config-if)#exit	Exit interface mode
#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process
(config-router)#address-family ipv4 unicast	Enable the IPv4 address family
(config-router-af)#redistribute connected	Redistribute the connected routes to generate external LSAs
(config-router-af)#summary-address 200.1.1.0/24	Summarize the external routes at the ASBR.

Validation

Validation 1: Verify that adjacency has been established with the configured instance identifier.

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (100-ABC)
Neighbor ID     Pri   State              Dead Time   Interface  Instance ID
10.12.49.123      1   Full/Backup     00:00:38       eth1       64
10.12.49.125      1   Full/DR            00:00:38       eth2       65
```

Validation 2: Verify that a single summarized OSPF IA route and a single summarized external route is available in FIB of R1

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.0.0.0/8 is directly connected, eth0, 00:45:18
C            11.1.1.0/24 is directly connected, eth1, 00:40:01
O IA         22.1.1.0/24 [110/2] via 11.1.1.2, eth1, 00:37:57
O IA         100.1.1.0/24 [110/2] via 11.1.1.2, eth1, 00:24:59
C            127.0.0.0/8 is directly connected, lo, 00:45:18
O E2         200.1.1.0/24 [110/20] via 11.1.1.2, eth1, 00:00:54

Gateway of last resort is not set
R1#
```

Validation 3: Verify that the Inter-Area Prefix LSA and External LSA in OSPFv3 database of R1 consists of just a single prefix 100.1.1.0/24 and 200.1.1.0/24 respectively

```
R1#show ipv6 ospf database inter-prefix
```

```
            OSPFv3 Router with ID (10.12.49.123) (Process 100-ABC)

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

  LS age: 771
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.124
  LS Seq Number: 0x80000002
  Checksum: 0x60E3
  Length: 32
    Metric: 1
    Prefix: 22.1.1.0/24
    Prefix Options: 0


  LS age: 21
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.12.49.124
  LS Seq Number: 0x80000008
  Checksum: 0x489D
  Length: 32
    Metric: 1
    Prefix: 127.0.0.0/8
    Prefix Options: 0


  LS age: 1795
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.5
  Advertising Router: 10.12.49.124
  LS Seq Number: 0x80000001
  Checksum: 0x975B
  Length: 32
    Metric: 1
    Prefix: 100.1.1.0/24
    Prefix Options: 0


R1#


R1#show ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.123) (Process 100-ABC)

                AS-external-LSA

  LS age: 390
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.125
  LS Seq Number: 0x80000001
  Checksum: 0xCE5A
  Length: 32
```

```
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 10.0.0.0/8
    Prefix Options: 0 (-|-|-|-)


  LS age: 364
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.4
  Advertising Router: 10.12.49.125
  LS Seq Number: 0x80000001
  Checksum: 0x6CE8
  Length: 32
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 200.1.1.0/24
    Prefix Options: 0 (-|-|-|-)


R1#
```

Validation 4: Verify that a single summarized external route is present in the ABR R2

```
R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.0.0.0/8 is directly connected, eth0, 00:55:15
C            11.1.1.0/24 is directly connected, eth1, 00:49:17
C            22.1.1.0/24 is directly connected, eth2, 00:48:18
O            100.1.1.0/24 [110/0] is a summary, Null, 00:35:05
C            100.1.1.100/32 is directly connected, lo, 00:35:40
C            100.1.1.110/32 is directly connected, lo, 00:35:36
C            127.0.0.0/8 is directly connected, lo, 00:55:15
O E2         200.1.1.0/24 [110/20] via 22.1.1.2, eth2, 00:11:00

Gateway of last resort is not set
R2#
```

Validation 5: Verify that the Type 5 LSA in the ABR's Link State Data Base consistes of just a single prefix 200.1.1.0/24

```
R2#show ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.124) (Process 100-ABC)

                AS-external-LSA

  LS age: 774
```

```
LS Type: AS-External-LSA
Link State ID: 0.0.0.1
Advertising Router: 10.12.49.125
LS Seq Number: 0x80000001
Checksum: 0xCE5A
Length: 32
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 10.0.0.0/8
  Prefix Options: 0 (-|-|-|-)


LS age: 748
LS Type: AS-External-LSA
Link State ID: 0.0.0.4
Advertising Router: 10.12.49.125
LS Seq Number: 0x80000001
Checksum: 0x6CE8
Length: 32
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 200.1.1.0/24
  Prefix Options: 0 (-|-|-|-)
```

Distribute List

To filter the routes that Open Shortest Path First Version 3 (OSPFv3) installs in the Routing Information Base (RIB), use the `distribute-list in` command in an appropriate configuration mode.

To filter the routes redistributed into Open Shortest Path First Version 3 (OSPFv3) from other routing protocols, use the `distribute-list out` command in an appropriate configuration mode.

Topology

Figure 5-29 shows the configuration to illustrate the distribute-list support for OSPFv3

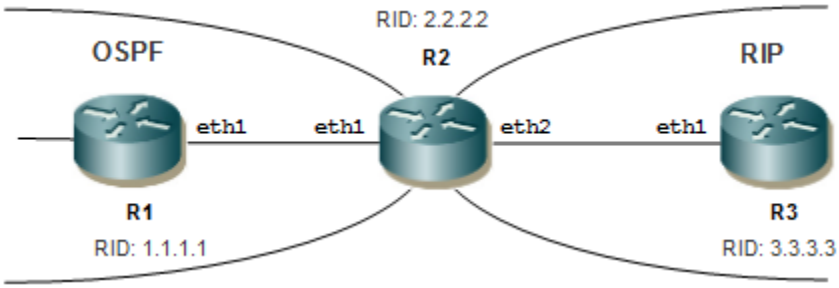


Figure 5-29: Basic Topology for Distribute-list

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::1/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)# ipv6 address 1111::1/128`	Configure the IPv6 address of the interface.
`(config-if)# ipv6 address 2222::2/128`	Configure the IPv6 address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf proc1`	Configure the routing process
`(config-router)#router-id 1.1.1.1`	Configure router-id to uniquely identify the router
`(config-router)#redistribute connected`	Redistribute connected routes into ospfv3
`(config-router)#end`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::50/64`	Configure the IPv6 address of the interface
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ipv6 address 4000::50/64`	Configure the IPv6 address of the interface.
`(config-if)#exit`	Exit interface mode
`(config-if)#ipv6 router rip`	Configure rip instance under interface
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 rip`	Configure the rip routing process
`(config-router)#neighbor fe80::5054:ff:fe85:19bc eth2`	Configure RIP neighbor peer
`(config-router)#exit`	Exit router mode.
`(config)#ipv6 access-list 1`	Configure ipv6 access list
`(config-ipv6-acl)# permit any 7777::/64 any`	Configure ipv6 access-list to permit 7777::/64 and deny 8888::/64
`(config-ipv6-acl)#exit`	Exit ipv6 access-list mode
`(config)#ipv6 access-list 2`	Configure ipv6 access-list
`(config-ipv6-acl)#permit any 1111::1/128 any`	Configure ipv6 access-list to permit 1111::1/128 and deny 2222::2/128
`(config-ipv6-acl)#exit`	Exit ipv6 access-list mode

(config)#router ipv6 ospf proc1	Configure the ospfv3 routing process
(config-router)#router-id 2.2.2.2	Configure router-id to uniquely identify the router
(config-router)#redistribute rip	Redistribute rip routes
(config-router)#distribute-list 1 out rip	Configure distribute list to allow only the permitted routes redistributed from RIP
(config-router)#distribute-list 2 in	Configure distribute list to allow the installation of only the permitted OSPFv3 routes in RIB
(config-router)#exit	Exit router mode
(config)#ipv6 access-list 1	Enter access-list mode
(config-ipv6-acl)#permit any 8888::/64 any	Configure the ipv6 access-list to permit 8888::/64 alongwith 7777::/64
(config-ipv6-acl)#exit	Exit access-list mode
(config)#ipv6 access-list 2	Enter access-list mode
(config-ipv6-acl)#permit any 2222::2/128 any	Configure the ipv6 access-list to permit 2222::2/128 alongwith 1111::1/128
(config-ipv6-acl)#exit	Exit access-list mode
(config)#exit	Exit configure mode

R3

#configure terminal	Enter configure mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 address 4000::51/64	Configure the IPv6 address of the interface.
(config-if)#ipv6 router rip	Configure rip instance under interface
(config-if)#exit	Exit interface mode
(config)#router ipv6 rip	Configure the rip routing process
(config-router)#neighbor fe80::5054:ff:fec6:69f eth1	Configure rip neighbor peer
(config-router)#end	Exit router mode
(config)#ipv6 route 7777::/64 eth2	Configure static route
(config)#ipv6 route 8888::/64 eth3	Configure static route
(config)#router ipv6 rip	Configure the rip routing process
(config-router)#redistribute static	Redistribute configured static routes
(config-router)#end	Exit router mode

Validation 1

Verify OSPF neighborship is up between R1and R2

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (Proc1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:38    eth1       0
```

Validation 2

Check if permitted route 7777::/64 is present in R1's routing table and denied route 8888::/64 is not present.

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
   Destination     Metric           Next-hop
C  2000::/64         1             directly connected, eth1, Area 0.0.0.0
E2 7777::/64        1/20   via    fe80::5054:ff:fe1e:269d, eth1
```

Validation 3

Check both the routes 7777::/64 and 8888::/64 are present after 8888::/64 is permitted

R1

```
rtr1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination    Metric    Next-hop
C  2000::/64         1      directly connected, eth1, Area 0.0.0.0
E2 7777::/64        1/20   via fe80::5054:ff:fe1e:269d, eth1
E2 8888::/64        1/20   via fe80::5054:ff:fe1e:269d, eth1
```

Validation 4

Check if permitted route 1111::1/128 is present in R2's routing table and denied route 2222::2/128 is not present.

R1

```
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:43:35
O E2   1111::1/128 [110/20] via fe80::5054:ff:fe0c:40ed, eth1, 00:01:17
C      2000::/64 via ::, eth1, 00:36:33
C      4000::/64 via ::, eth2, 00:36:19
R      7777::/64 [120/2] via fe80::5054:ff:fe96:a3f9, eth2, 00:21:57
R      8888::/64 [120/2] via fe80::5054:ff:fe96:a3f9, eth2, 00:21:57
C      fe80::/64 via ::, eth9, 00:43:35
R2#
```

Validation 5

Check both the routes 1111::1/128 and 2222::2/128 are present after 2222::2/128 is permitted.

R1

```
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:54:52
O E2   1111::1/128 [110/20] via fe80::5054:ff:fe0c:40ed, eth1, 00:12:34
C      2000::/64 via ::, eth1, 00:47:50
O E2   2222::2/128 [110/20] via fe80::5054:ff:fe0c:40ed, eth1, 00:00:02
C      4000::/64 via ::, eth2, 00:47:36
R      7777::/64 [120/2] via fe80::5054:ff:fe96:a3f9, eth2, 00:33:14
R      8888::/64 [120/2] via fe80::5054:ff:fe96:a3f9, eth2, 00:33:14
C      fe80::/64 via ::, eth9, 00:54:52
```

CHAPTER 6 IS-IS IPv4

This chapter contains basic IS-IS (Intermediate System to Intermediate System) configuration examples.

Enable IS-IS on an Interface

This example shows the minimum configuration required for enabling IS-IS on an interface. R1 and R2 are two routers in the ABC instance connecting to the network 10.10.10.0/24. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

Topology

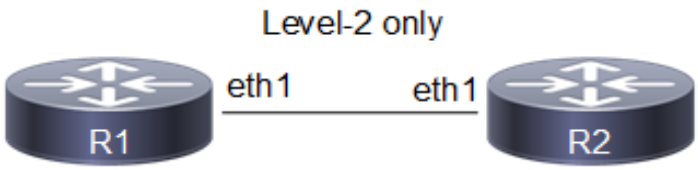


Figure 6-30: Basic IS-IS Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).

`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     24        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0001.01

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      21.21.21.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds

R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
```

```
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.002a.230a
    IP interface address:
      21.21.21.1/24
    IPv6 interface address:
      fe80::5054:ff:fe2a:230a/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 1 seconds

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    21.21.21.0/24       10          --                  eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    21.21.21.0/24       10          --                  eth1            0

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1
5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000009   0x6C2D        980               0/0/0
```

```
0000.0000.0001.01-00* 0x00000003   0x1DBB        980               0/0/0
0000.0000.0002.00-00  0x0000000A   0x5444        980               0/0/0
0000.0000.0002.01-00  0x00000005   0xE113        0 (978)           0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000009   0x6C2D        942               0/0/0
0000.0000.0001.01-00  0x00000003   0x1DBB        942               0/0/0
0000.0000.0002.00-00* 0x0000000A   0x5444        944               0/0/0
    0000.0000.0002.01-00* 0x00000005   0xE113        0 (941)           0/0/0
```

Set Priority

This example describes how to set the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R3 is configured to have a priority of 70, this is higher than the default priority (64) of R1 and R2. This makes R3 the DIS.

Topology

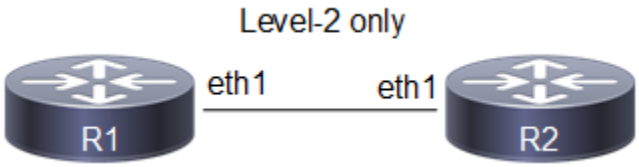


Figure 6-31: Set IS-IS Priority

Configuration

R1

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).

`(config-if)#isis priority 125`	Specify the router priority to a higher priority (125) to make R2 the designated IS (DIS).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     6         L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     21        L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   125       0000.0000.0002.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0002.01

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      21.21.21.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

```
R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.002a.230a
    IP interface address:
      21.21.21.1/24
    IPv6 interface address:
      fe80::5054:ff:fe2a:230a/64
    Level-2 Metric: 10/10, Priority: 125, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 737 milliseconds
```

Dynamic hostname

This example shows how to configure Dynamic Hostname for an ISIS instance. Dynamic hostname is the method of mapping name-to-systemID. It allows the routing protocol to advertise symbolic names in the IS-IS PDUs. This is done by the addition of a new TLV which allows the IS-IS routers to include the name-to-systemID mapping data in their LSPs. This allows for simple and reliable transport of name mapping across IS-IS networks. Dynamic hostname can be either the hostname of the node or the tag of the configured ISIS instance.

Note: Dynamic-hostname has to be configured on all nodes for it to take effect.

Topology

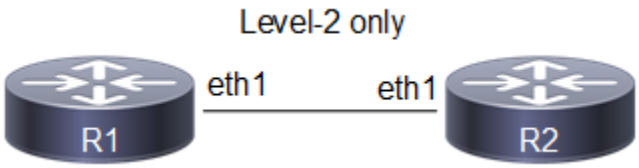


Figure 6-32: Basic dynamic hostname topology

Configuration

R1

(config)#interface eth1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config)#ip address 21.21.21.2/24	Configure IP address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.

R2

(config)#interface eth1	Enter interface mode.
(config)#ip address 21.21.21.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        5254.002a.230a  Up     28        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76  Up     7         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```

```
R2             eth1        Up     L2   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R1             eth1        Up     L2   64        0000.0000.0001.01

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000B   0x1D6B        1170              0/0/0
R1.01-00            * 0x00000004   0x1BBC        538               0/0/0
R2.00-00              0x0000000C   0x0D79        1166              0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x0000000B   0x1D6B        1078              0/0/0
R1.01-00              0x00000004   0x1BBC        445               0/0/0
R2.00-00            * 0x0000000C   0x0D79        1075              0/0/0
```

Redistribute Routes into IS-IS

In this example, the configuration causes OSPF routes to be imported into the IS-IS routing table, and advertised into the ABC instance.

Topology

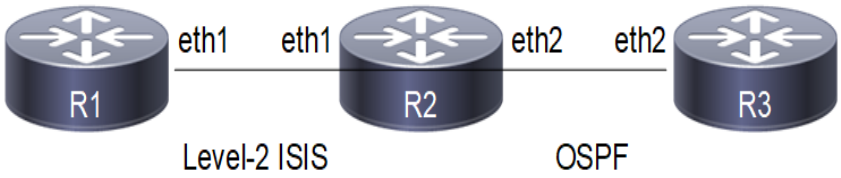


Figure 6-33: Redistribute Routes Into IS-IS

Configuration

R1

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.

R2

`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config)#ip address 31.31.31.1/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#redistribute ospf`	Specify redistributing routes from other routing protocol (OSPF) into IS-IS.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#exit`	Exit interface mode.
`(config)#interface lo`	Configure interface lo
`(config-if)#ip address 2.2.2.2/32 secondary`	Configure secondary IP address to loopback interface
`(config-if)#exit`	Exit interface mode.

(config)#router ospf 100	Configure OSPF routing process and specify the tag (100) which uniquely identifies the routing process
(config-router)#ospf router-id 2.2.2.2	Specify a Router ID (2.2.2.2) for the OSPF routing process.
(config-router)#network 2.2.2.2/32 area 0.0.0.0	Advertising 2.2.2.2 network
(config-router)#network 31.31.31.0/24 area 0.0.0.0	Advertising 31 network
(config-router)#exit	Exit router mode.

R3

(config)#interface eth2	Enter interface mode.
(config)#ip address 31.31.31.2/24	Configure IP address on interface.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Configure interface lo
(config-if)#ip address 3.3.3.3/32 secondary	Configure secondary IP address to loopback interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure OSPF routing process and specify the tag (100) which uniquely identifies the routing process
(config-router)#ospf router-id 3.3.3.3	Specify a Router ID (3.3.3.3) for the OSPF routing process.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertising 3.3.3.3 network
(config-router)#network 31.31.31.0/24 area 0.0.0.0	Advertising 31 network

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        5254.002a.230a      Up     25        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76      Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R2             eth1        Up     L2   64        0000.0000.0001.01
```

```
R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R1             eth1        Up     L2   64        0000.0000.0001.01

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000003   0x2D63        1096              0/0/0
R1.01-00            * 0x00000002   0x1FBA        1096              0/0/0
R2.00-00              0x00000004   0xEF02        1108              0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000003   0x2D63        1021              0/0/0
R1.01-00              0x00000002   0x1FBA        1021              0/0/0
R2.00-00            * 0x00000004   0xEF02        1035              0/0/0


R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   2.2.2.2/32          10          21.21.21.1          eth1            0
L2   3.3.3.3/32          10          21.21.21.1          eth1            0
C    21.21.21.0/24       10          --                  eth1            0
L2   31.31.31.0/24       10          21.21.21.1          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

```
Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
E    2.2.2.2/32          0           --                  --             0
E    3.3.3.3/32          0           --                  --             0
C    21.21.21.0/24       10          --                  eth1            0
E    31.31.31.0/24       0           --                  --             0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L2         2.2.2.2/32 [115/10] via 21.21.21.1, eth1, 00:16:54
i L2         3.3.3.3/32 [115/10] via 21.21.21.1, eth1, 00:16:43
C            10.12.30.0/24 is directly connected, eth0, 00:24:28
C            21.21.21.0/24 is directly connected, eth1, 00:18:37
i L2         31.31.31.0/24 [115/10] via 21.21.21.1, eth1, 00:16:54
C            127.0.0.0/8 is directly connected, lo, 00:24:28

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            2.2.2.2/32 is directly connected, lo, 00:21:31
O            3.3.3.3/32 [110/2] via 31.31.31.2, eth2, 00:20:14
C            10.12.30.0/24 is directly connected, eth0, 00:27:36
C            21.21.21.0/24 is directly connected, eth1, 00:21:31
C            31.31.31.0/24 is directly connected, eth2, 00:21:31
C            127.0.0.0/8 is directly connected, lo, 00:27:36

Gateway of last resort is not set

R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
3.3.3.3          1   Full/Backup    00:00:35   31.31.31.2      eth2
0
```

```
R3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:32    31.31.31.1      eth2
0

R2#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, LP - Link Protecting,
       NP - Node Protecting, BID - Broadcast Link Protecting

C  2.2.2.2/32 [1] is directly connected, lo, Area 0.0.0.0
O  3.3.3.3/32 [2] via 31.31.31.2, eth2, Area 0.0.0.0
C  31.31.31.0/24 [1] is directly connected, eth2, Area 0.0.0.0

R3#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, LP - Link Protecting,
       NP - Node Protecting, BID - Broadcast Link Protecting

O  2.2.2.2/32 [2] via 31.31.31.1, eth2, Area 0.0.0.0
C  3.3.3.3/32 [1] is directly connected, lo, Area 0.0.0.0
C  31.31.31.0/24 [1] is directly connected, eth2, Area 0.0.0.0

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O            2.2.2.2/32 [110/2] via 31.31.31.1, eth2, 00:19:47
C            3.3.3.3/32 is directly connected, lo, 00:20:40
C            10.12.30.0/24 is directly connected, eth0, 00:26:28
C            31.31.31.0/24 is directly connected, eth2, 00:20:40
C            127.0.0.0/8 is directly connected, lo, 00:26:28

Gateway of last resort is not set
```

Metric

You can make a route the preferred route by changing its metric. In this example, the cost has been configured to make R3 the next hop for R1.

The default metric for each interface is 10. Interface eth3 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+20 = 30

R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 10.10.14.0/24.

Topology

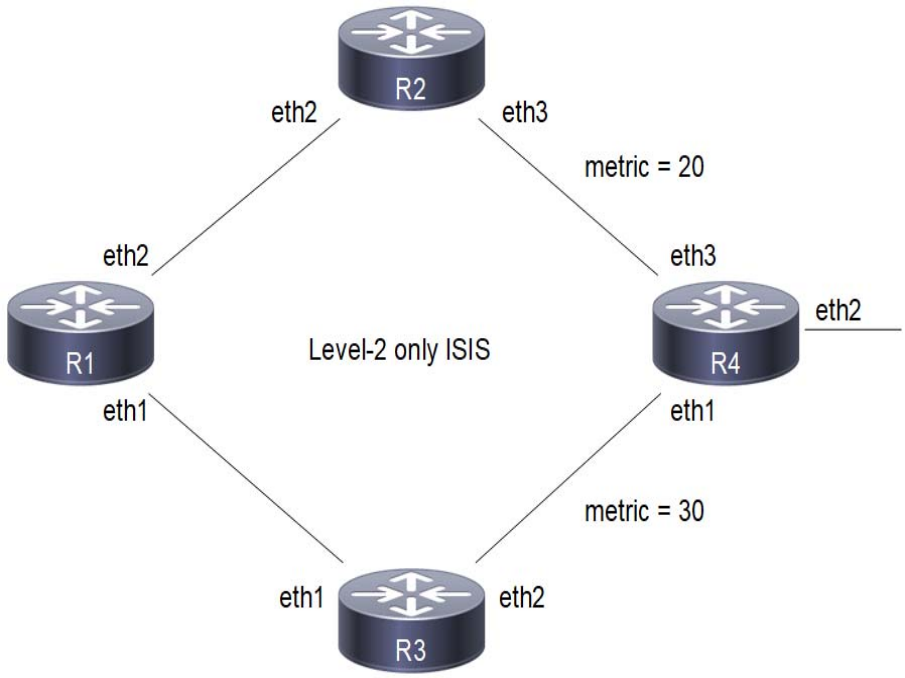


Figure 6-34: Configure IS-IS Metric

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.

(config-if)#ip address 30.30.30.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.30.30.2/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 40.40.40.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 20	Set the value of IS-IS metric (on eth2) to 20.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth1	Enter interface mode.
(config-if)#ip address 20.20.20.2/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#ip address 50.50.50.1/24	Configure IP address on interface.
(config-if)#isis metric 30	Set the value of IS-IS metric (on eth2) to 30.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#ip address 50.50.50.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#ip address 40.40.40.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R3             eth1        5254.00dc.2f11  Up     5         L2   IS-IS
R2             eth2        5254.007e.5ade  Up     20        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth2        5254.00a1.6afe  Up     7         L2   IS-IS
R4             eth3        5254.00b1.d6fb  Up     8         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76  Up     20        L2   IS-IS
R4             eth2        5254.00f5.35a4  Up     8         L2   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
```

```
Tag ABC:  VRF : default
System Id      Interface   SNPA                State  Holdtime  Type Protocol
R3             eth1        5254.00a8.940d      Up     25        L2   IS-IS
R2             eth3        5254.0049.c509      Up     25        L2   IS-IS

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth2        5254.007e.5ade
R3                   10         R3       eth1        5254.00dc.2f11
R4                   30         R2       eth2        5254.007e.5ade

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth2        5254.00a1.6afe
R2                   --
R3                   20         R1       eth2        5254.00a1.6afe
R4                   20         R4       eth3        5254.00b1.d6fb

R3#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   20         R1       eth1        5254.00dc.0b76
R3                   --
R4                   30         R4       eth2        5254.00f5.35a4

R4#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   20         R2       eth3        5254.0049.c509
                                R3       eth1        5254.00a8.940d
R2                   10         R2       eth3        5254.0049.c509
R3                   10         R3       eth1        5254.00a8.940d
R4                   --

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
L2   40.40.40.0/24       30          30.30.30.2          eth2            0
```

```
L2   50.50.50.0/24       40          30.30.30.2          eth2            0
                                     20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0
C    40.40.40.0/24       20          --                  eth3            0
L2   50.50.50.0/24       30          40.40.40.2          eth3            0


R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
L2   30.30.30.0/24       20          20.20.20.1          eth1            0
L2   40.40.40.0/24       40          20.20.20.1          eth1            0
                                     50.50.50.2          eth2            0
C    50.50.50.0/24       30          --                  eth2            0

R4#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          50.50.50.1          eth1            0
L2   30.30.30.0/24       20          40.40.40.1          eth3            0
C    40.40.40.0/24       10          --                  eth3            0
C    50.50.50.0/24       10          --                  eth1            0

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      20.20.20.1/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
```

```
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 5 seconds
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.00a1.6afe
    IP interface address:
      30.30.30.1/24
    IPv6 interface address:
      fe80::5054:ff:fea1:6afe/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 183 milliseconds

R2#show isis interface
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.007e.5ade
    IP interface address:
      30.30.30.2/24
    IPv6 interface address:
      fe80::5054:ff:fe7e:5ade/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 706 milliseconds
eth3 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000005
    Local SNPA: 5254.0049.c509
    IP interface address:
      40.40.40.1/24
    IPv6 interface address:
      fe80::5054:ff:fe49:c509/64
    Level-2 Metric: 20/10, Priority: 64, Circuit ID: 0000.0000.0004.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 2 seconds

R3#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
```

```
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.2f11
    IP interface address:
      20.20.20.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:2f11/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 2 seconds
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.00a8.940d
    IP interface address:
      50.50.50.1/24
    IPv6 interface address:
      fe80::5054:ff:fea8:940d/64
    Level-2 Metric: 30/10, Priority: 64, Circuit ID: 0000.0000.0004.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 3 seconds

R4#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00f5.35a4
    IP interface address:
      50.50.50.2/24
    IPv6 interface address:
      fe80::5054:ff:fef5:35a4/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0004.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds
eth3 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000005
    Local SNPA: 5254.00b1.d6fb
    IP interface address:
      40.40.40.2/24
    IPv6 interface address:
      fe80::5054:ff:feb1:d6fb/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0004.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
        Next IS-IS LAN Level-2 Hello in 0 milliseconds
```


L1-L2 Area Routing with a Single Instance

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the single-instance version of the Level-1-2 router.

Topology

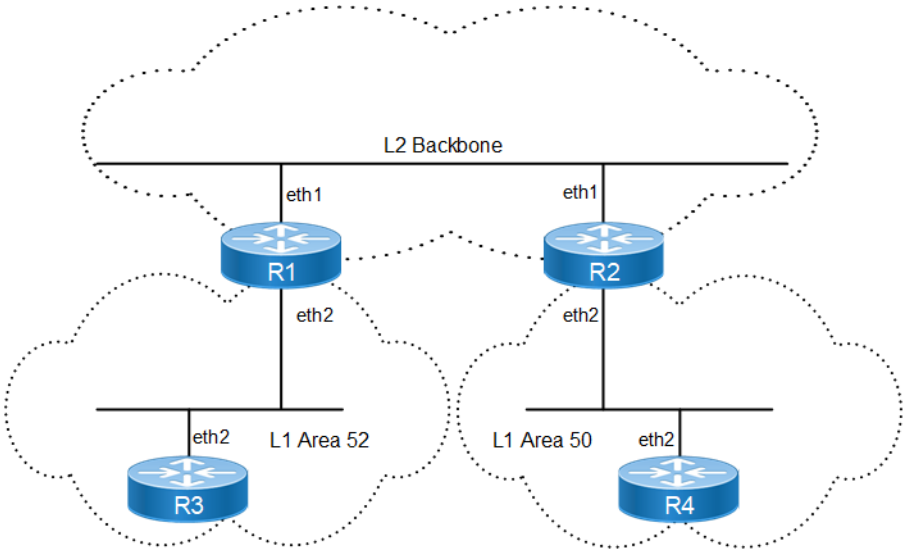


Figure 6-35: Single-Instance L1-L2 Area Routing

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on the interface `eth0` for area ABC.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type for the interface `eth0`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on the interface `eth1` for area ABC.
`(config-if)#isis circuit-type level-1`	Set the circuit type for interface `eth1` to level 1.
`(config-if)#exit`	Exit interface mode.

`#configure terminal`	Enter configure mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area ABC.
`(config-router)#net 52.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis bb`	Enable IS-IS routing on the interface `eth0` for area `bb`.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type for the interface `eth0` to level-2 only.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.1/24`	Configure IP address on interface.
`(config-if)#ip router isis bb`	Enable IS-IS routing on interface `eth1` for area `bb`.
`(config-if)#isis circuit-type level-1`	Set the circuit type for interface `eth1` to level 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis bb`	Create an IS-IS routing instance for area `bb`.
`(config-router)#net 50.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#ip router isis xyz`	Enable IS-IS routing on the interface `eth0` for area `xyz`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis xyz`	Create an IS-IS routing instance for area `xyz`.
`(config-router)#is-type level-1`	Set the IS level for this area (`xyz`) as `level-1`.
`(config-router)#net 52.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.2/24`	Configure IP address on interface.
`(config-if)#ip router isis aa`	Enable IS-IS routing on the interface `eth0` for area `aa`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis aa`	Create an IS-IS routing instance for area `aa`.
`(config-router)#is-type level-1`	Set the IS level for this area (`aa`) as `level-1`.
`(config-router)#net 50.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     20        L2   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     6         L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag bb:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     8         L2   IS-IS
0000.0000.0004 eth2        5254.00e2.aece  Up     7         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag xyz:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.00a1.6afe  Up     23        L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag aa:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade  Up     25        L1   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
L2   40.40.40.0/24       20          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag bb:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
L2   30.30.30.0/24       20          20.20.20.1          eth1            0
C    40.40.40.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag xyz:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   0.0.0.0/0           10          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R4#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag aa:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   0.0.0.0/0           10          40.40.40.1          eth2            0
C    40.40.40.0/24       10          --                  eth2            0

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       --
0000.0000.0003       10         0000.0000.0003      eth2
5254.00a8.940d

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002      eth1
5254.002a.230a

R2#show isis topology

Tag bb:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0002       --
0000.0000.0004       10         0000.0000.0004      eth2
5254.00e2.aece

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
```

```
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R3#show isis topology

Tag xyz:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth2
5254.00a1.6afe
0000.0000.0003       --

R4#show isis topology

Tag aa:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       10         0000.0000.0002       eth2
5254.007e.5ade
0000.0000.0004       --

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 00:27:08
C            20.20.20.0/24 is directly connected, eth1, 00:16:57
C            30.30.30.0/24 is directly connected, eth2, 00:15:48
i L2         40.40.40.0/24 [115/20] via 20.20.20.2, eth1, 00:15:05
C            127.0.0.0/8 is directly connected, lo, 00:27:08

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 00:27:17
C            20.20.20.0/24 is directly connected, eth1, 00:17:13
i L2         30.30.30.0/24 [115/20] via 20.20.20.1, eth1, 00:16:18
C            40.40.40.0/24 is directly connected, eth2, 00:15:36
C            127.0.0.0/8 is directly connected, lo, 00:27:17
```

```
Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 30.30.30.1 to network 0.0.0.0

i*L1         0.0.0.0/0 [115/10] via 30.30.30.1, eth2, 00:16:47
C            10.12.30.0/24 is directly connected, eth0, 00:27:46
C            30.30.30.0/24 is directly connected, eth2, 00:16:52
C            127.0.0.0/8 is directly connected, lo, 00:27:46

R4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 40.40.40.1 to network 0.0.0.0

i*L1         0.0.0.0/0 [115/10] via 40.40.40.1, eth2, 00:16:26
C            10.12.30.0/24 is directly connected, eth0, 00:27:20
C            40.40.40.0/24 is directly connected, eth2, 00:16:36
C            127.0.0.0/8 is directly connected, lo, 00:27:20

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000005   0xE66E        1165              1/0/0
0000.0000.0003.00-00  0x00000004   0xDC80        1164              0/0/0
0000.0000.0003.01-00  0x00000002   0x10C8        1163              0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000005   0xD0D8        1148              0/0/0
0000.0000.0001.01-00* 0x00000002   0x1FBA        1109              0/0/0
0000.0000.0002.00-00  0x00000005   0x7219        1189              0/0/0

R2#show isis database
Tag bb:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```

```
0000.0000.0002.00-00* 0x00000005   0x9583        1179              1/0/0
0000.0000.0004.00-00  0x00000004   0x8B95        1177              0/0/0
0000.0000.0004.01-00  0x00000002   0x2FA6        1177              0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000005   0xD0D8        1116              0/0/0
0000.0000.0001.01-00  0x00000002   0x1FBA        1078              0/0/0
0000.0000.0002.00-00* 0x00000005   0x7219        1160              0/0/0

R3#show isis database
Tag xyz:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000005   0xE66E        1094              1/0/0
0000.0000.0003.00-00* 0x00000004   0xDC80        1095              0/0/0
0000.0000.0003.01-00* 0x00000002   0x10C8        1094              0/0/0

R4#show isis database
Tag aa:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000005   0x9583        1105              1/0/0
0000.0000.0004.00-00* 0x00000004   0x8B95        1105              0/0/0
0000.0000.0004.01-00* 0x00000002   0x2FA6        1105              0/0/0
```

L1-L2 Area Routing with Multiple Instances

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the multiple-instance version of the Level-1-2 router.

Topology

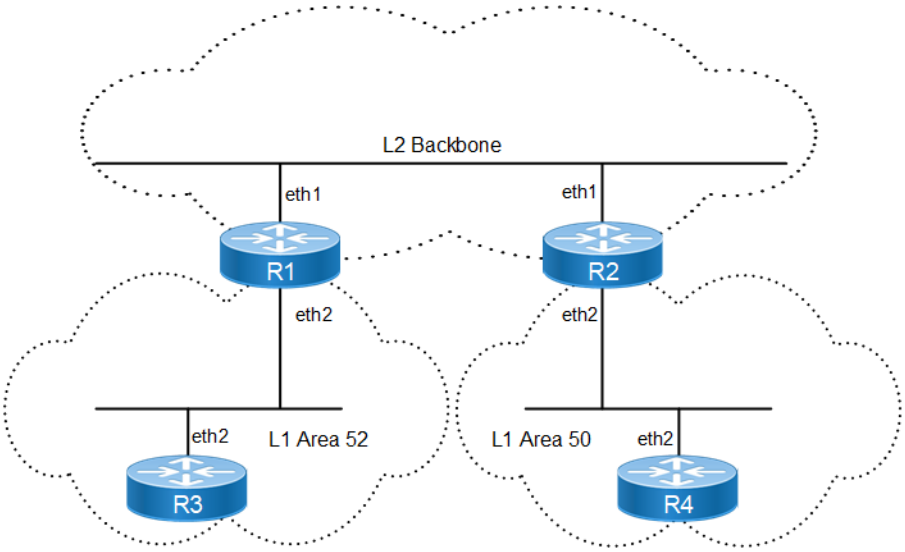


Figure 6-36: Multiple-Instance L1-L2 Area Routing

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis aaa`	Enable IS-IS routing on interface `eth0` for area `aaa`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis aaa`	Create an IS-IS routing instance for area `aaa`.
`(config-router)#is-type level-2-only`	Set the IS level for this area (`aaa`) as `level-2-only`.
`(config-router)#net bb.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ccc`	Enable IS-IS routing on interface `eth1` for area `ccc`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ccc`	Create an IS-IS routing instance for area `ccc`.
`(config-router)#is-type level-1`	Set the IS level for this area (`ccc`) as `level-1`.
`(config-router)#net cc.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis bb`	Enable IS-IS routing on interface `eth0` for area `bb.`
`(config-if)#exit`	Exit interface mode.
`(config)#router isis bb`	Create an IS-IS routing instance for area `bb`.
`(config-router)#is-type level-2-only`	Set the IS level for this area (`bb`) as `level-2-only`.
`(config-router)#net bb.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on interface `eth1` for area ABC.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area ABC.
`(config-router)#is-type level-1`	Set the IS level for this area (ABC) as `level-1`.
`(config-router)#net cc.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#ip router isis xyz`	Enable IS-IS routing on interface `eth0` for area `xyz`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis xyz`	Create an IS-IS routing instance for area `xyz`.
`(config-router)#is-type level-1`	Set the IS level for this area (`xyz`) as `level-1`.
`(config-router)#net 52.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.2/24`	Configure IP address on interface.
`(config-if)#ip router isis aa`	Enable IS-IS routing on interface `eth0` for area `aa`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis aa`	Create an IS-IS routing instance for area `aa`.
`(config-router)#is-type level-1`	Set the IS level for this area (`aa`) as `level-1`.
`(config-router)#net 52.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag aaa:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     25        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ccc:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag bb:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag aaa:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   64        0000.0000.0001.01

Tag ccc:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id

Tag bb:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0001.01

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

```
Tag aaa:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0


Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ccc:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    30.30.30.0/24       10          --                  eth2            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    40.40.40.0/24       10          --                  eth2            0


Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag bb:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0

R1#show isis topology

Tag aaa:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1
5254.002a.230a


Tag ccc:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       --

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0003       --


Tag bb:  VRF : default
IS-IS paths to level-2 routers
```

```
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R1#show isis database
Tag aaa:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000002   0x181D        1003              0/0/0
0000.0000.0001.01-00* 0x00000001   0x21B9        1003              0/0/0
0000.0000.0002.00-00  0x00000005   0x1818        1080              0/0/0

Tag ccc:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000001   0xDFA5        685               0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0003.00-00* 0x00000002   0xD571        696               0/0/0

Tag bb:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x181D        938               0/0/0
0000.0000.0001.01-00  0x00000001   0x21B9        938               0/0/0
0000.0000.0002.00-00* 0x00000005   0x1818        1017              0/0/0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 01:37:50
C            20.20.20.0/24 is directly connected, eth1, 00:10:13
C            30.30.30.0/24 is directly connected, eth2, 00:10:13
C            127.0.0.0/8 is directly connected, lo, 01:37:50

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
```

```
        * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 01:37:26
C            20.20.20.0/24 is directly connected, eth1, 00:05:03
C            40.40.40.0/24 is directly connected, eth2, 00:08:52
C            127.0.0.0/8 is directly connected, lo, 01:37:26

Gateway of last resort is not set
```

Route Leaking

Route leaking is defined in RFC 2966. For Level-1 (L1) routers, only level-1 routes are populated in the routing table. The L1 router has a default route to the nearest Level-1/Level-2 (L1/L2) router: This could result in sub-optimal routing in certain scenarios. Route leaking causes an L1/L2 router to advertise the level-2 routes in its database to the L1 router, thus allowing the L1 router to acknowledge the prefixes advertised by the Level-2 (L2) router. In this way, the L1 router has the ability to learn the true cost to reach other areas.

In the following example, R1 is the L1 router, R2 is the L1/L2 router doing the route leaking, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacency with R1 and R3 are already up, and the route tables with appropriate routes are already populated.

Topology

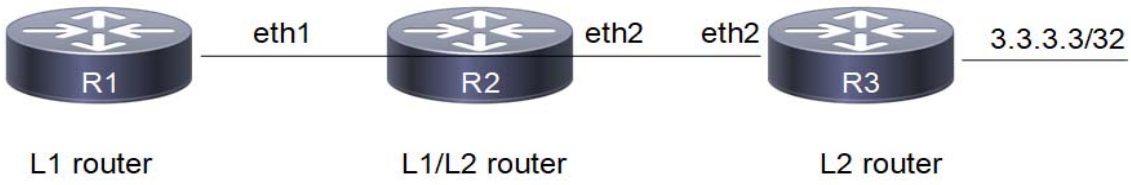


Figure 6-37: Route Leaking Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#is-type level-1`	Configure instance as level-1.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R1).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth2 (connected to R3).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0002.00`	Define the NET address.
`(config-router-af)#redistribute isis level-2 into level-1`	Enable redistribution of isis routes from level-2 into level-1

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface (lo)to configure and enter Interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Configure IP address on loopback interface.
`(config-if)# ip router isis 1`	Enable IS-IS routing on interface lo
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0003.00`	Define the NET address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type as level-2-only for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

In the example, route, `i ia 3.3.3.3/32 [115/30] via 20.20.20.2, eth1, 00:12:29`, is the L2 route leaked by the L1/L2 router into the L1 router.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a      Up     21        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76      Up     5         L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d      Up     6         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade      Up     21        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
ia   3.3.3.3/32          30          20.20.20.2          eth1            0
C    20.20.20.0/24       10          --                  eth1            0
L1   30.30.30.0/24       20          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
```

```
L2   3.3.3.3/32          20          30.30.30.2          eth2            0
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    3.3.3.3/32          10          --                  lo            0
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i ia         3.3.3.3/32 [115/30] via 20.20.20.2, eth1, 00:20:53
C            10.12.30.0/24 is directly connected, eth0, 01:02:10
C            20.20.20.0/24 is directly connected, eth1, 00:48:08
i L1         30.30.30.0/24 [115/20] via 20.20.20.2, eth1, 00:23:30
C            127.0.0.0/8 is directly connected, lo, 01:02:10

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L2         3.3.3.3/32 [115/20] via 30.30.30.2, eth2, 00:21:07
C            10.12.30.0/24 is directly connected, eth0, 01:01:55
C            20.20.20.0/24 is directly connected, eth1, 00:48:12
C            30.30.30.0/24 is directly connected, eth2, 00:48:12
```

```
C            127.0.0.0/8 is directly connected, lo, 01:01:55

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            3.3.3.3/32 is directly connected, lo, 00:21:25
C            10.12.30.0/24 is directly connected, eth0, 01:01:26
i L2         20.20.20.0/24 [115/20] via 30.30.30.1, eth2, 00:24:06
C            30.30.30.0/24 is directly connected, eth2, 00:48:13
C            127.0.0.0/8 is directly connected, lo, 01:01:26

Gateway of last resort is not set

R1#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x0000000C   0xE4B5        642               0/0/0
0000.0000.0001.01-00* 0x00000007   0x13C3        642               0/0/0
0000.0000.0002.00-00  0x00000012   0x8AC8        804               0/0/0

R2#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000C   0xE4B5        624               0/0/0
0000.0000.0001.01-00  0x00000007   0x13C3        624               0/0/0
0000.0000.0002.00-00* 0x00000012   0x8AC8        787               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x0000000E   0x0380        765               0/0/0
0000.0000.0003.00-00  0x00000006   0xB702        785               0/0/0
0000.0000.0003.01-00  0x00000004   0x27AC        615               0/0/0

R3#show isis database
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x0000000E   0x0380        727               0/0/0
```

```
0000.0000.0003.00-00* 0x00000006   0xB702        750               0/0/0
0000.0000.0003.01-00* 0x00000004   0x27AC        579               0/0/0

R1#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1        5254.002a.230a

R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1        5254.00dc.0b76
0000.0000.0002       --

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       --
0000.0000.0003       10         0000.0000.0003       eth2        5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       10         0000.0000.0002       eth2        5254.007e.5ade
0000.0000.0003       --
```

Route Summarization

Route summarization makes the routing table smaller, but still allows complete IP connectivity, if everything is configured properly.

The following example consists of a three-router topology, in which R2 is doing the summarization. In this example, R1 is the L1 router, R2 is the L1/L2 router doing the summarization, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacencies with R1 and R3 are already up, and the route tables with the appropriate routes are already populated.

Topology

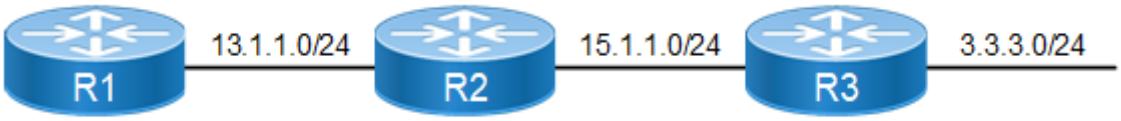


Figure 6-38: Route Summarization Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#is-type level-1`	Configure instance as level-1.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R1).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type as level-2-only for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth2 (connected to R3).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0002.00`	Define the NET address.

(config-router-af)#redistribute isis level-2 into level-1	Enable redistribution of isis routes from level-2 into level-1
(config-router-af)# summary-address 90.0.0.0/6 level-1 metric 50	Configure the summary address to summarize IP reachability information.

R3

#configure terminal	Enter configure mode.
(config)#ip route 66.66.66.1/24 eth2	Configure ip static route.
(config)#ip route 77.77.77.1/24 eth2	Configure ip static route.
(config)#ip route 88.88.88.1/24 eth2	Configure ip static route.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0001.0000.0000.0003.00	Define the NET address.
(config-router)#redistribute static	Enable redistribution of static routes into ISIS instance.
(config-router)#exit	Exit router mode.
(config)#interface eth2	Specify the interface (eth2)to configure and enter Interface mode.
(config-if)#ip address 30.30.30.2/24	Configure IP address on interface.
(config-if)#isis circuit-type level-2-only	Set the circuit type as level-2-only for the interface
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R2).

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     20        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     7         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
```

```
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade      Up     21        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
ia   30.30.30.0/24       20          20.20.20.2          eth1            0
ia   66.66.66.1/32       20          20.20.20.2          eth1            0
ia   77.77.77.1/32       20          20.20.20.2          eth1            0
ia   88.0.0.0/6          60          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
L2   66.66.66.1/32       10          30.30.30.2          eth2            0
L2   77.77.77.1/32       10          30.30.30.2          eth2            0
D    88.0.0.0/6          0           --                  --
L2   88.88.88.1/32       10          30.30.30.2          eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0
E    66.66.66.1/32       0           --                  --             0
E    77.77.77.1/32       0           --                  --             0
E    88.88.88.1/32       0           --                  --             0

R1#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000003   0xF6AC        680               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
```

```
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00* 0x00000002   0x1DBE        680               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000006   0xA58B        1048              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
  Metric:   10         IP-Interarea 30.30.30.0 255.255.255.0
  Metric:   10         IP-External 66.66.66.1     255.255.255.255
  Metric:   10         IP-External 77.77.77.1     255.255.255.255
  Metric:   50         IP-External 88.0.0.0     252.0.0.0

R2#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000003   0xF6AC        655               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00  0x00000002   0x1DBE        655               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000006   0xA58B        1025              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
  Metric:   10         IP-Interarea 30.30.30.0 255.255.255.0
  Metric:   10         IP-External 66.66.66.1     255.255.255.255
  Metric:   10         IP-External 77.77.77.1     255.255.255.255
  Metric:   50         IP-External 88.0.0.0     252.0.0.0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000004   0x1776        667               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0003.00-00  0x00000004   0x2257        890               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   0          IP-External 66.66.66.1     255.255.255.255
  Metric:   0          IP-External 77.77.77.1     255.255.255.255
```

```
  Metric:   0          IP-External 88.88.88.1     255.255.255.255
0000.0000.0003.01-00  0x00000002   0x2BAA        666               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R3#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000004   0x1776        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0003.00-00* 0x00000004   0x2257        868               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   0          IP-External 66.66.66.1     255.255.255.255
  Metric:   0          IP-External 77.77.77.1     255.255.255.255
  Metric:   0          IP-External 88.88.88.1     255.255.255.255
0000.0000.0003.01-00* 0x00000002   0x2BAA        645               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00
```

IS-IS Distance

Administrative distance in IS-IS can be configured for a specified source ID or for all routes.

This example shows configuring the IS-IS administrative distance for the IPv4 address family.

Topology

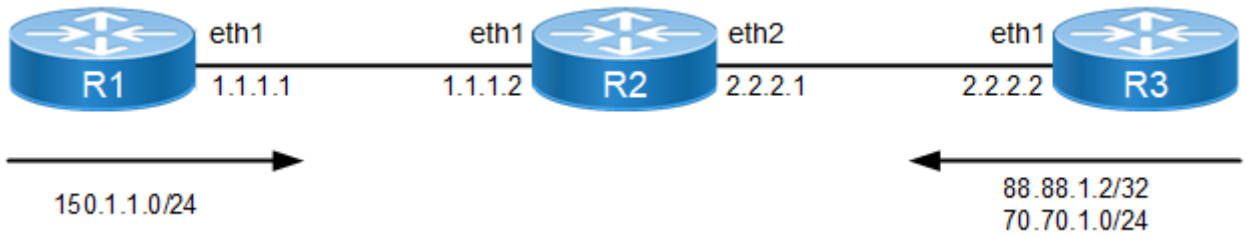


Figure 6-39: IS-IS Distance Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/24`	Assign the IP address on this interface (`eth1`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1`.
`(config)#ip route 150.1.1.0/24 eth1`	Configure static routes.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0001.00`	Set a Network Entity Title (NET) for this instance, specifying the address and the system ID.
`(config-router)#redistribute static`	Redistribute the static routes.

R2

`#configure terminal`	Enter configure mode
`(config)#ip access-list DIST`	Enter access list mode
`(config-ip-acl)#permit ipip 88.88.1.2/32 any`	Create an access list to permit the `88.88.1.2/32` route from R3.
`(config-ip-acl)#exit`	Exit access list mode
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 1.1.1.2/24`	Assign the IP address on this interface (`eth1`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1`
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 2.2.2.1/24`	Assign the IP address on this interface (`eth2`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth2`
`(config-if)#exit`	Exit interface mode
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0002.00`	Specify the NET address.
`(config-router)#distance 100`	Configure the administrative distance for all routes received from R1 and R2.
`(config-router)#distance 20 0001.0000.0001`	Configure the administrative distance for all routes received from R1. This command overwrites the applied distance, 100, and will apply distance 20 for all routes received from R1.
`(config-router)#distance 30 0001.0000.0003 DIST`	Configure the distance, `30`, to the route, 88.88.1.2/32, received from R3. All other routes from R3 (for example, 70.70.1.0/24) will have the distance applied as 100. If the distance, 100, is not configured, all other routes will have a default distance of 115.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/24`	Assign the IP address on this interface (`eth1`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 88.88.1.2/32 eth2`	Configure static routes
`(config)#ip route 70.70.1.0/24 eth2`	Configure static routes
`(config)#router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)#net 49.0001.0000.0003.00`	Specify the NET address.
`(config-router)#redistribute static`	Redistribute the static routes.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0002 eth1        5254.002a.230a  Up     18        L1   IS-IS
                                           Up     18        L2   IS-IS
R2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0001 eth1        5254.00dc.0b76  Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
0001.0000.0003 eth2        5254.00a8.940d  Up     8         L1   IS-IS
                                           Up     8         L2   IS-IS
R3#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0002 eth2        5254.007e.5ade  Up     20        L1   IS-IS
                                           Up     20        L2   IS-IS
R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
```

```
C    1.1.1.0/24          10          --                  eth1            0
L1   2.2.2.0/24          20          1.1.1.2             eth1            0
L2   70.70.1.0/24        20          1.1.1.2             eth1            0
L2   88.88.1.2/32        20          1.1.1.2             eth1            0
E    150.1.1.0/24        0           --                  --             0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    1.1.1.0/24          10          --                  eth1            0
C    2.2.2.0/24          10          --                  eth2            0
L2   70.70.1.0/24        10          2.2.2.2             eth2            0
L2   88.88.1.2/32        10          2.2.2.2             eth2            0
L2   150.1.1.0/24        10          1.1.1.1             eth1            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   1.1.1.0/24          20          2.2.2.1             eth2            0
C    2.2.2.0/24          10          --                  eth2            0
E    70.70.1.0/24        0           --                  --             0
E    88.88.1.2/32        0           --                  --             0
L2   150.1.1.0/24        20          2.2.2.1             eth2            0



R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.0/24 is directly connected, eth1, 00:30:56
i L1         2.2.2.0/24 [115/20] via 1.1.1.2, eth1, 00:26:01
C            10.12.30.0/24 is directly connected, eth0, 00:33:46
i L2         70.70.1.0/24 [115/20] via 1.1.1.2, eth1, 00:21:39
i L2         88.88.1.2/32 [115/20] via 1.1.1.2, eth1, 00:15:04
C            127.0.0.0/8 is directly connected, lo, 00:33:46
S            150.1.1.0/24 [1/0] is directly connected, eth1, 00:29:03

Gateway of last resort is not set
```

```
R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.0/24 is directly connected, eth1, 00:26:46
C            2.2.2.0/24 is directly connected, eth2, 00:26:30
C            10.12.30.0/24 is directly connected, eth0, 00:33:21
i L2         70.70.1.0/24 [100/10] via 2.2.2.2, eth2, 00:21:55
i L2         88.88.1.2/32 [30/10] via 2.2.2.2, eth2, 00:15:09
C            127.0.0.0/8 is directly connected, lo, 00:33:21
i L2         150.1.1.0/24 [20/10] via 1.1.1.1, eth1, 00:25:53

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L1         1.1.1.0/24 [115/20] via 2.2.2.1, eth2, 00:22:56
C            2.2.2.0/24 is directly connected, eth2, 00:23:01
C            10.12.30.0/24 is directly connected, eth0, 00:33:57
S            70.70.1.0/24 [1/0] is directly connected, eth2, 00:23:01
S            88.88.1.2/32 [1/0] is directly connected, eth2, 00:16:07
C            127.0.0.0/8 is directly connected, lo, 00:33:57
i L2         150.1.1.0/24 [115/20] via 2.2.2.1, eth2, 00:22:42

Gateway of last resort is not set

R1#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000003   0x2AEC        448               0/0/0
0001.0000.0001.01-00* 0x00000002   0x32A4        448               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        698               0/0/0
0001.0000.0003.00-00  0x00000006   0xE820        702               0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        698               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000008   0xB20F        703               0/0/0
0001.0000.0001.01-00* 0x00000002   0x32A4        448               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        698               0/0/0
```

```
0001.0000.0003.00-00  0x0000000A   0xB2CE        1108              0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        698               0/0/0

R2#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000003   0x2AEC        402               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        401               0/0/0
0001.0000.0002.00-00* 0x00000004   0x5A80        653               0/0/0
0001.0000.0003.00-00  0x00000006   0xE820        656               0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        652               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000008   0xB20F        657               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        401               0/0/0
0001.0000.0002.00-00* 0x00000004   0x5A80        653               0/0/0
0001.0000.0003.00-00  0x0000000A   0xB2CE        1062              0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        652               0/0/0

R3#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000003   0x2AEC        317               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        317               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        568               0/0/0
0001.0000.0003.00-00* 0x00000006   0xE820        573               0/0/0
0001.0000.0003.01-00* 0x00000002   0x3E94        569               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000008   0xB20F        573               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        317               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        568               0/0/0
0001.0000.0003.00-00* 0x0000000A   0xB2CE        979               0/0/0
    0001.0000.0003.01-00* 0x00000002   0x3E94        569               0/0/0

R1#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       --
0001.0000.0002       10         0001.0000.0002       eth1
5254.002a.230a
0001.0000.0003       20         0001.0000.0002       eth1
5254.002a.230a

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       --
0001.0000.0002       10         0001.0000.0002       eth1
5254.002a.230a
0001.0000.0003       20         0001.0000.0002       eth1
5254.002a.230a
```

```
R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       10         0001.0000.0001       eth1
5254.00dc.0b76
0001.0000.0002       --
0001.0000.0003       10         0001.0000.0003       eth2
5254.00a8.940d

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       10         0001.0000.0001       eth1
5254.00dc.0b76
0001.0000.0002       --
0001.0000.0003       10         0001.0000.0003       eth2
5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       20         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0002       10         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0003       --

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       20         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0002       10         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0003       --
```

Passive Interface

In ISP and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the Default Passive-Interface feature, there were two possibilities for obtaining routing information from all of these interfaces:

- Configure a routing protocol on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive, which was time consuming.

The solution to this problem was to configure the routing protocol on all interfaces and manually set the `passive-interface` command on the interfaces where adjacency was not desired. In certain networks, this meant coding 200 or more passive-interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single `passive-interface` default command, then configuring individual interfaces in which adjacencies are desired using the `no passive-interface <interface-name>` command.

Usage

1. When a specific interface is configured as passive using the `passive-interface <interface-name>` command:
   - The interface loses its adjacency on that interface, for example, eth1.
   - The interface (eth1) is still advertised by other IS-IS speaking interfaces to their neighbors.
2. When a specific interface is configured as passive using `passive-interface <interface-name>` command followed by removing the configuration using `no passive-interface <interface-name>` command:
   - The interface is IS-IS disabled and must be enabled using the `ip router isis` command (for example, `ip router isis 1`).
   - If IS-IS is not configured, the interface (for example, eth1) will not be advertised by other IS-IS speaking interfaces to their neighbors.
3. When an interface is configured with the `passive interface` command:
   - All IS-IS enabled interfaces lose their adjacency.
   - All IS-IS enabled interfaces in the system will be made passive.
   - To establish adjacency on a particular interface, `no passive interface <interface-name>`" command must be enabled.
   - All interfaces which were made passive are advertised by the active IS-IS speaking interface to its neighbors.
4. When an interface is configured with the `no passive interface` command:
   - All interfaces which are currently passive, will become active.
   - If IS-IS is configured on those interface, it will start sending out IS-IS packets and attempt to form adjacency.
   - If IS-IS is not configured on those interfaces, it will not be advertised by the active IS-IS speaking interface to its neighbors.

Topology

Figure 6-40 shows a passive-interface configuration example.

Figure 6-40: IS-IS Passive Interface

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.

(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Specify the interface (eth1)to configure and enter Interface mode.
(config-if)#ip address 20.20.20.1/24	Configure IP address on interface.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R2).

R2

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1)to configure and enter Interface mode.
(config-if)#ip address 20.20.20.2/24	Configure IP address on interface.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R1).
(config-if)#exit	Exit interface mode and return to Configure mode.
(config)#interface eth2	Specify the interface (eth2)to configure and enter Interface mode.
(config-if)#ip address 30.30.30.1/24	Configure IP address on interface.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2 (connected to R3).
(config-if)#exit	Exit interface mode and return to Configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0002.00	Define the NET address.
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#passive-interface eth1	Configure the eth1 interface as passive.

R3

#configure terminal	Enter configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0001.0000.0000.0003.00	Define the NET address.
(config-router)#exit	Exit router mode.
(config)#interface eth2	Specify the interface (eth2)to configure and enter Interface mode.
(config-if)#ip address 30.30.30.2/24	Configure IP address on interface.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R2).

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
```

```
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2        5254.00a8.940d  Up     9         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade  Up     19        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       0           --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       10          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R1#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```

```
0000.0000.0001.00-00* 0x00000004   0x3A02        1069              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00* 0x00000001   0xF108        0 (1068)          0/0/0

R2#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x3EFF        852               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0002.00-00* 0x00000003   0x3761        869               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IP 20.20.20.0 255.255.255.0
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.00-00  0x00000002   0x530E        872               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.01-00  0x00000001   0x2DA9        868               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R3#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x3EFF        767               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0002.00-00  0x00000003   0x3761        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IP 20.20.20.0 255.255.255.0
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.00-00* 0x00000002   0x530E        788               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.01-00* 0x00000001   0x2DA9        784               0/0/0
  Metric:   0          IS 0000.0000.0003.00
```

```
  Metric:   0          IS 0000.0000.0002.00

R1# show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --

R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       **
0000.0000.0002       --
0000.0000.0003       10         0000.0000.0003       eth2
5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       **
0000.0000.0002       10         0000.0000.0002       eth2
5254.007e.5ade
0000.0000.0003       --
```

IS-IS IPv4 Loop-Free Alternate Fast Reroute

This section contains IS-IS (Intermediate System to Intermediate System) Loop-Free Alternate Fast Reroute (LFA-FRR) configuration examples.

For details about the commands used in these examples, see the *Intermediate System to Intermediate System Command Reference*.

OSPF LFA and ISIS LFA along with MPLS is not supported. Do not configure OSPF LFA or ISIS LFA, if MPLS is configured or vice-versa.

Overview

When a primary next-hop fails, LFA-FRR reduces the failure reaction time to tens of milliseconds using a pre-computed alternate next- hop, so that the alternate can be rapidly used when the failure is detected. A network with this feature experiences less traffic loss and less micro-looping of packets than a network without LFA-FRR.

After you enable LFA-FRR, routers calculate a backup path for each primary path to reach the destination. The backup path is calculated based on the attributes such as node protecting, link protecting, and broadcast link protecting. If there is an ECMP path to reach prefixes, the backup is selected from the same primary set by default; if a secondary tie-breaker is enabled, and if a secondary path is available, the backup will be selected from the secondary path.

Basic Configuration

Topology

Figure 6-41 shows the configuration to enable the basic ISIS LFA feature.

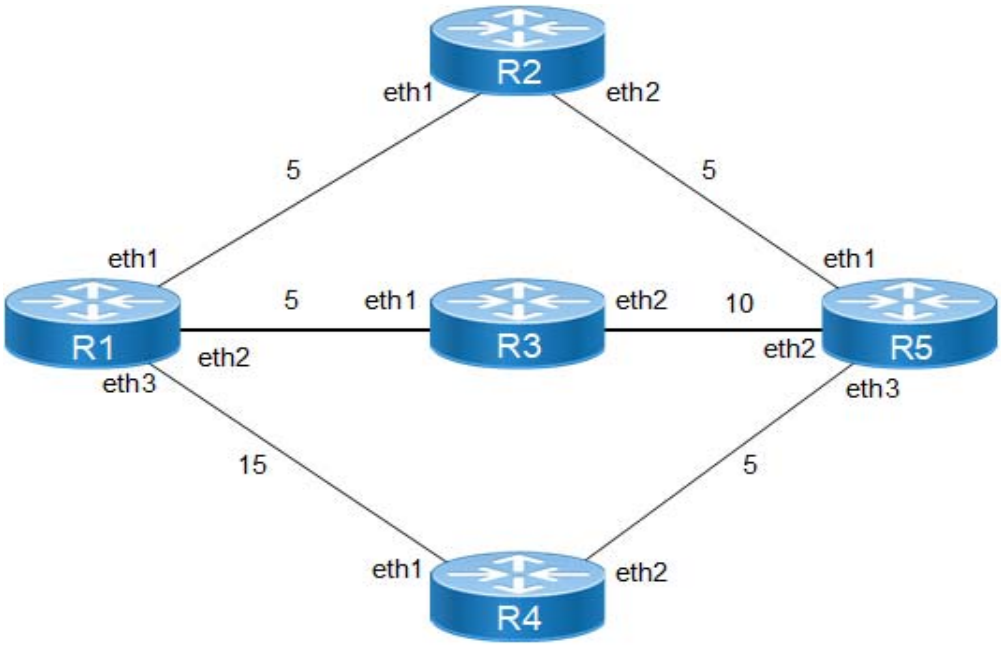


Figure 6-41: ISIS LFA-FRR

R1

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 10.10.10.142/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 20.20.20.142/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 30.30.30.142/24`	Configure the IP address of the interface.

(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 15	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#fast-reroute per-prefix level-1 proto ipv4 all	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learnt
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R2

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.10.10.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.40.40.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R3

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 20.20.20.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1

(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.50.50.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R4

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 30.30.30.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 15	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 60.60.60.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0004.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R5

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 40.40.40.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 50.50.50.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 60.60.60.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)#net 49.0000.0000.0005.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

R1

ISIS neighborship:

```
R1#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     27        L1   IS-IS
0000.0000.0003 eth2        5254.00dc.2f11  Up     7         L1   IS-IS
0000.0000.0004 eth3        5254.00f5.35a4  Up     7         L1   IS-IS
```

```
R2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L1   IS-IS
0000.0000.0005 eth2        5254.00b3.110c  Up     7         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00a1.6afe  Up     22        L1   IS-IS
0000.0000.0005 eth2        5254.0056.7a3d  Up     27        L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.0011.a028  Up     21        L1   IS-IS
0000.0000.0005 eth2        5254.00d3.fb41  Up     21        L1   IS-IS


R5#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.007e.5ade  Up     27        L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     6         L1   IS-IS
0000.0000.0004 eth3        5254.00e2.aece  Up     7         L1   IS-IS
```

Check the ISIS route installation with primary and backup paths in the ISIS table and RIB table.

Primary paths:

```
R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    10.10.10.0/24       5           --                  eth1            0
C    20.20.20.0/24       5           --                  eth2            0
C    30.30.30.0/24       15          --                  eth3            0
```

```
    L1   40.40.40.0/24       10          10.10.10.141        eth1            0
    L1   50.50.50.0/24       15          20.20.20.143        eth2            0
    L1   60.60.60.0/24       15          10.10.10.141        eth1            0

    R1#show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
           ia - IS-IS inter area, E - EVPN,
           v - vrf leaked
           * - candidate default

    IP Route Table for VRF "default"
    C            10.10.10.0/24 is directly connected, eth1, 00:43:14
    C            10.12.30.0/24 is directly connected, eth0, 01:42:55
    C            20.20.20.0/24 is directly connected, eth2, 00:43:14
    C            30.30.30.0/24 is directly connected, eth3, 00:43:14
    i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:16:42
    i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:16:55
    i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:16:42
    C            127.0.0.0/8 is directly connected, lo, 01:42:55

    Gateway of last resort is not set
```

R1#FRR backup paths:

```
    R1#show ip isis route fast-reroute

    Tag   : 1  VRF : default
    Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
            D - discard, LP - Link Protecting, NP - Node Protecting,
            BP - Broadcast Interface Disjoint, Pri - Primary Path,
            Sec - Secondary Path, DP - Downstream Path

    L1  40.40.40.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 25
        Protection Provided : LP NP BP

    L1  50.50.50.0/24
        Primary Path via    : 20.20.20.143, eth2
        FRR Backup Path via : 10.10.10.141, eth1
        FRR Metric          : 20
        Protection Provided : LP NP BP

    L1  60.60.60.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 20
        Protection Provided : LP NP BP DP

    R1#show ip route fast-reroute
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:18:01
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:18:14
                      [FRR-NH] via 10.10.10.141, eth1

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:18:01
                      [FRR-NH] via 30.30.30.144, eth3
```

It is not mandatory that for all primary paths, there exists an LFA backup path only if inequality equation satisfies according to attributes configured on routers, backup path will be calculated.

To prohibit an interface from being used as a repair path, disable fast reroute calculation on the interface:

`R1(config-if)#interface eth1`	Enter interface.
`(config-if)# isis fast-reroute per-prefix candidate disable level-1`	Disable fast reroute calculation on the interface.
`(config-if)#end`	Exit.

Verify that the `eth2` interface is not used for backup path calculation.

```
R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

L1  50.50.50.0/24
    Primary Path via    : 20.20.20.143, eth2
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  60.60.60.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:20:22
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:20:35
                      [FRR-NH] via 30.30.30.144, eth3

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:20:22
                      [FRR-NH] via 30.30.30.144, eth3

R1#
```

Backup Path based on Route-Map Prefixes

R1

Route-map and access-list configuration:

`(config)#ip access-list 1`	Create an access-list
`(config-ip-acl)#permit any 40.40.40.0 0.0.0.255 any`	Configuring rule to permit only one prefix
`(config)#route-map rmap1 permit 1`	Create a route-map
`(config-route-map)#match ip address 1`	Apply above created access-list in route-map
`(config)#exit`	Exit config mode.

Apply the above created route-map with fast-reroute:

`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)#fast-reroute per-prefix level-1 proto ipv4 route-map rmap1`	Configure LFA-FRR to calculate the available backup path for routes allowed through route-map
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
```

```
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:02:04
C            10.12.30.0/24 is directly connected, eth0, 02:01:45
C            20.20.20.0/24 is directly connected, eth2, 01:02:04
C            30.30.30.0/24 is directly connected, eth3, 01:02:04
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:35:32
i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:35:45
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:35:32
C            127.0.0.0/8 is directly connected, lo, 02:01:45

Gateway of last resort is not set

R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:35:48
                      [FRR-NH] via 30.30.30.144, eth3  FRR Table has only
allowed prefix through route-map , for remaining prefixes, FRR not present
```

LFA Tie-Breaker

Based on the index values configured, if inequalities are satisfied, protections will be provided:

- Lower the index will have the highest priority, The path which provides protection with highest priority will be selected. If there are multiple paths providing the highest priority protection then we will check which of the path provides the protection which has 2nd highest priority and so on.
- If all the paths provide same priority, then the LFA route is chosen on the basis of path cost.
- If none of the paths provides the protection with highest priority, then we will see which path provides the 2nd highest priority and so on.

The show command below displays default values for tie-breaker, by default maximum protection (link, node, broadcast, if ecmp, ecmp backup path) will be provided.

After configuring tie-breaker with index, values will be changed accordingly.

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-----------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 60
 Node Protecting              : 30
 Broadcast Interface Disjoint : 70
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms
```

R1

To change index values, below configurations should be used, with the lower the index highest the priority.

`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)#fast-reroute per-prefix level-1 proto ipv4 all`	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learned
`(config-router)#fast-reroute tie-break level-1 proto ipv4 interface-disjoint index 1`	Configure index value to change priority for link protection
`(config-router)#fast-reroute tie-break level-1 proto ipv4 node-protecting index 2`	Configure index value to change priority for node protection
`(config-router)#fast-reroute tie-break level-1 proto ipv4 broadcast-interface-disjoint index 3`	Configure index value to change priority for broadcast link protection
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-----------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 1
 Node Protecting              : 2
 Broadcast Interface Disjoint : 3
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms
```

```
    R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

L1  50.50.50.0/24
    Primary Path via    : 20.20.20.143, eth2
    FRR Backup Path via : 10.10.10.141, eth1
    FRR Metric          : 20
    Protection Provided : LP NP BP

L1  60.60.60.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:45:16
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:45:29
                      [FRR-NH] via 10.10.10.141, eth1

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:45:16
                      [FRR-NH] via 30.30.30.144, eth3
```

LFA Termination

A router MUST limit the amount of time an alternate next-hop is used after the primary next-hop has become unavailable. This ensures that the router will start using the new primary next-hops.

LFA termination avoids a micro looping in topology, when particular network goes down, LFA backup path will be installed and if termination interval is configured, LFA backup will be still used till the interval and it is used in order to verify new primary path is loop free.

R1

Configure termination interval on R1 in router mode:

(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#fast-reroute terminate-hold-on interval 100000	Configure LFA termination interval
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-------------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 1
 Node Protecting              : 2
 Broadcast Interface Disjoint : 3
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 100000 ms

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:19:46
C            10.12.30.0/24 is directly connected, eth0, 02:19:27
C            20.20.20.0/24 is directly connected, eth2, 01:19:46
C            30.30.30.0/24 is directly connected, eth3, 01:19:46
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:53:14
i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:53:27
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:53:14
C            127.0.0.0/8 is directly connected, lo, 02:19:27

Gateway of last resort is not set
```

Shut down one of the primary nexthops, here eth2 of R1:

(config)#interface eth2	Enter interface mode
(config-if)#shutdown	Shutdown the interface

(config-if)#exit	Exit interface mode
(config)exit	Exit config mode

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     27        L1   IS-IS
0000.0000.0004 eth3        5254.00f5.35a4  Up     7         L1   IS-IS
```

Here, eth1 has become a primary path, which was originally a backup path:

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:24:47
C            10.12.30.0/24 is directly connected, eth0, 02:24:28
i L1         20.20.20.0/24 [115/25] via 10.10.10.141, eth1, 00:02:01
C            30.30.30.0/24 is directly connected, eth3, 01:24:47
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:02:01
i L1         50.50.50.0/24 [115/20] via 10.10.10.141, eth1, 00:02:01
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:02:01
C            127.0.0.0/8 is directly connected, lo, 02:24:28

Gateway of last resort is not set

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    10.10.10.0/24       5           --                  eth1            0
L1   20.20.20.0/24       25          10.10.10.141        eth1            0
C    30.30.30.0/24       15          --                  eth3            0
L1   40.40.40.0/24       10          10.10.10.141        eth1            0
L1   50.50.50.0/24       20          10.10.10.141        eth1            0
L1   60.60.60.0/24       15          10.10.10.141        eth1            0

R1#show ip isis route fast-reroute
```

```
    Tag   : 1  VRF : default
    Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
            D - discard, LP - Link Protecting, NP - Node Protecting,
            BP - Broadcast Interface Disjoint, Pri - Primary Path,
            Sec - Secondary Path, DP - Downstream Path

    L1  20.20.20.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 35
        Protection Provided : LP NP BP DP

    L1  40.40.40.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 25
        Protection Provided : LP NP BP

    L1  50.50.50.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 30
        Protection Provided : LP NP BP DP

    L1  60.60.60.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 20
        Protection Provided : LP NP BP DP

    R1#show ip route fast-reroute
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
    area ,p - stale info
           * - candidate default

    IP Route Table for VRF "default"
    i L1    20.20.20.0/24 [115/25] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3

    i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3

    i L1    50.50.50.0/24 [115/20] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3

    i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3
```

LFA For ECMP Paths

Equal-Cost Multi-Path Routing (ECMP) is a routing technique where next-hop packet forwarding to a single destination can occur over multiple “best-paths” that tie in routing metric calculations. Because it is a per-hop decision limited to a single router, it can increase bandwidth by load-balancing traffic over multiple paths.

Here, we provide configuration capabilities for Loop-Free Alternate (LFA) Fast Reroute (FRR) along with ECMP.

Topology

Figure 6-42 shows the configuration to enable the ISIS LFA feature with ECMP.

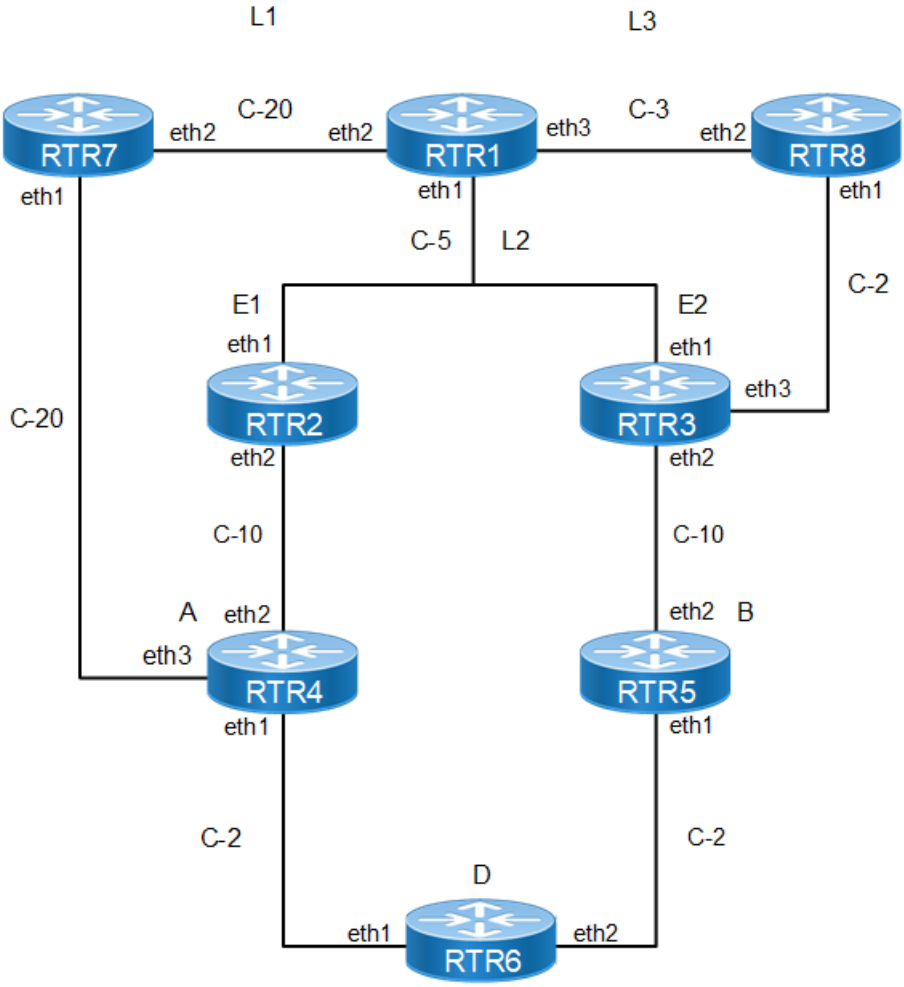


Figure 6-42: ISIS LFA-FRR ECMP

RTR1, S

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 10.1.1.142/24`	Configure the IP address of the interface.

(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 20.1.1.142/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 20	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth3	Enter interface mode.
(config-if)#ip address 30.1.1.142/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 3	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#fast-reroute per-prefix level-1 proto ipv4 all	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learnt
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR2

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.1.1.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.1.1.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1

(config-router)#net 49.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR3

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.1.1.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.1.1.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth3	Enter interface mode.
(config-if)#ip address 60.1.1.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR4

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 70.1.1.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface

(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.1.1.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth3	Enter interface mode.
(config-if)#ip address 80.1.1.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 20	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0004.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR5

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 90.1.1.145/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.1.1.145/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0005.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces

(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR6

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 70.1.1.146/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 90.1.1.146/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int lo	Enter interface mode.
(config-if)#ip address 146.146.146.146/32 secondary	Configure the IP address on the loopback interface
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0006.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR7

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 80.1.1.147/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 20	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.

(config-if)#ip address 20.1.1.147/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 20	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0007.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

RTR8

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 60.1.1.148/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 2	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 30.1.1.148/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 3	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0008.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

Validation

R (Source):

The backup path will be selected by default from same Primary/ECMP set and “Pri” indicates backup selected from ECMP set.

```
R1#show clns neighbors

Total number of L1 adjacencies: 4
```

```
Total number of L2 adjacencies: 0
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     22        L1   IS-IS
0000.0000.0003 eth1        5254.00dc.2f11  Up     6         L1   IS-IS
0000.0000.0007 eth2        5254.0098.a69e  Up     25        L1   IS-IS
0000.0000.0008 eth3        5254.00ed.c0d5  Up     6         L1   IS-IS

R2#show clnss  neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     29        L1   IS-IS
0000.0000.0003 eth1        5254.00dc.2f11  Up     8         L1   IS-IS
0000.0000.0004 eth2        5254.00e2.aece  Up     8         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 4
Total number of L2 adjacencies: 0
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     26        L1   IS-IS
0000.0000.0002 eth1        5254.002a.230a  Up     21        L1   IS-IS
0000.0000.0005 eth2        5254.0056.7a3d  Up     24        L1   IS-IS
0000.0000.0008 eth3        5254.009f.0dc5  Up     22        L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0006 eth1        5254.0044.d2cb  Up     27        L1   IS-IS
0000.0000.0002 eth2        5254.007e.5ade  Up     27        L1   IS-IS
0000.0000.0007 eth3        5254.00f7.8f87  Up     7         L1   IS-IS

R5#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0006 eth1        5254.00c6.d9ab  Up     8         L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     7         L1   IS-IS

R6#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
```

```
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth1        5254.00f5.35a4  Up     6         L1   IS-IS
0000.0000.0005 eth2        5254.00b3.110c  Up     27        L1   IS-IS

R7#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth1        5254.00b1.d6fb  Up     28        L1   IS-IS
0000.0000.0001 eth2        5254.00a1.6afe  Up     8         L1   IS-IS

R8#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.0011.a028  Up     22        L1   IS-IS
0000.0000.0003 eth3        5254.00b3.5aa3  Up     6         L1   IS-IS

R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.1.1.0/24
    Primary Path via    : 10.1.1.141, eth1
    FRR Backup Path via : 20.1.1.147, eth2
    FRR Metric          : 50
    Protection Provided : LP NP BP

L1  50.1.1.0/24
    Primary Path via    : 30.1.1.148, eth3
    FRR Backup Path via : 10.1.1.143, eth1
    FRR Metric          : 15
    Protection Provided : LP NP BP Pri DP ' Here Pri indicates backup selected
from ECMP set

    Primary Path via    : 10.1.1.143, eth1
    FRR Backup Path via : 30.1.1.148, eth3
    FRR Metric          : 15
    Protection Provided : LP BP Pri DP

L1  60.1.1.0/24
    Primary Path via    : 30.1.1.148, eth3
    FRR Backup Path via : 10.1.1.143, eth1
    FRR Metric          : 7
    Protection Provided : LP NP BP DP
```



```
L1  70.1.1.0/24
    Primary Path via    : 10.1.1.141, eth1
    FRR Backup Path via : 30.1.1.148, eth3
    FRR Metric          : 19
    Protection Provided : LP NP BP DP

L1  80.1.1.0/24
    Primary Path via    : 10.1.1.141, eth1
    FRR Backup Path via : 20.1.1.147, eth2
    FRR Metric          : 40
    Protection Provided : LP NP BP DP

L1  90.1.1.0/24
    Primary Path via    : 30.1.1.148, eth3
    FRR Backup Path via : 10.1.1.143, eth1
    FRR Metric          : 17
    Protection Provided : LP NP BP Pri DP

    Primary Path via    : 10.1.1.143, eth1
    FRR Backup Path via : 30.1.1.148, eth3
    FRR Metric          : 17
    Protection Provided : LP BP Pri DP

L1  146.146.146.146/32
    Primary Path via    : 30.1.1.148, eth3
    FRR Backup Path via : 10.1.1.141, eth1
    FRR Metric          : 27
    Protection Provided : LP NP BP Pri DP

    Primary Path via    : 10.1.1.143, eth1
    FRR Backup Path via : 10.1.1.141, eth1
    FRR Metric          : 27
    Protection Provided : NP Pri DP

    Primary Path via    : 10.1.1.141, eth1
    FRR Backup Path via : 30.1.1.148, eth3
    FRR Metric          : 27
    Protection Provided : LP NP BP Pri DP

R1# show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.1.1.0/24 [115/15] via 10.1.1.141, eth1, 00:13:33
                    [FRR-NH] via 20.1.1.147, eth2

i L1    50.1.1.0/24 [115/15] via 10.1.1.143, eth1, 00:16:25
                    [FRR-NH] via 30.1.1.148, eth3

                   [115/15] via 30.1.1.148, eth3
```

```
                      [FRR-NH] via 10.1.1.143, eth1

i L1    60.1.1.0/24 [115/5] via 30.1.1.148, eth3, 00:16:25
                    [FRR-NH] via 10.1.1.143, eth1

i L1    70.1.1.0/24 [115/17] via 10.1.1.141, eth1, 00:13:33
                    [FRR-NH] via 30.1.1.148, eth3

i L1    80.1.1.0/24 [115/35] via 10.1.1.141, eth1, 00:13:33
                    [FRR-NH] via 20.1.1.147, eth2

i L1    90.1.1.0/24 [115/17] via 10.1.1.143, eth1, 00:16:25
                    [FRR-NH] via 30.1.1.148, eth3

                   [115/17] via 30.1.1.148, eth3
                    [FRR-NH] via 10.1.1.143, eth1

i L1    146.146.146.146/32 [115/27] via 10.1.1.141, eth1, 00:02:18
                           [FRR-NH] via 30.1.1.148, eth3

                          [115/27] via 10.1.1.143, eth1
                           [FRR-NH] via 10.1.1.141, eth1

                          [115/27] via 30.1.1.148, eth3
                           [FRR-NH] via 10.1.1.141, eth1
```

Backup Path for ECMP Path from Non-ECMP Path

To select Backup path from secondary/Non-ECMP path, configure the below command in R1 with lowest index value.

If no backup path available from non-ecmp set , then from primary set itself , backup path will be installed

`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)#net 49.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#fast-reroute tie-break level-1 proto ipv4 secondary-path index 1`	Configure secondary path tie-breaker to select backup path from Non-ECMP path
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-----------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 60
 Node Protecting              : 30
 Broadcast Interface Disjoint : 70
 Secondary Path               : 1
 Downstream Path              : 90
```

```
     Termination Hold On Interval : 1000 ms
```

R1#Below, “Sec” indicates the backup path is from the Non-ECMP path

```
     R1#show ip isis route fast-reroute

    Tag   : 1  VRF : default
    Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
            D - discard, LP - Link Protecting, NP - Node Protecting,
            BP - Broadcast Interface Disjoint, Pri - Primary Path,
            Sec - Secondary Path, DP - Downstream Path

    L1  40.1.1.0/24
        Primary Path via    : 10.1.1.141, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 50
        Protection Provided : LP NP BP

    L1  50.1.1.0/24
        Primary Path via    : 30.1.1.148, eth3
        FRR Backup Path via : 10.1.1.141, eth1
        FRR Metric          : 20
        Protection Provided : LP NP BP Sec  ' Sec indicates backup path is from
    Non-ecmp path

        Primary Path via    : 10.1.1.143, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 54
        Protection Provided : LP NP BP Sec

    L1  60.1.1.0/24
        Primary Path via    : 30.1.1.148, eth3
        FRR Backup Path via : 10.1.1.143, eth1
        FRR Metric          : 7
        Protection Provided : LP NP BP DP

    L1  70.1.1.0/24
        Primary Path via    : 10.1.1.141, eth1
        FRR Backup Path via : 30.1.1.148, eth3
        FRR Metric          : 19
        Protection Provided : LP NP BP DP

    L1  80.1.1.0/24
        Primary Path via    : 10.1.1.141, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 40
        Protection Provided : LP NP BP DP

    L1  90.1.1.0/24
        Primary Path via    : 30.1.1.148, eth3
        FRR Backup Path via : 10.1.1.141, eth1
        FRR Metric          : 19
        Protection Provided : LP NP BP Sec DP

        Primary Path via    : 10.1.1.143, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 44
```

```
        Protection Provided : LP NP BP Sec

    L1  146.146.146.146/32
        Primary Path via    : 30.1.1.148, eth3
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 52
        Protection Provided : LP NP BP Sec

        Primary Path via    : 10.1.1.143, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 52
        Protection Provided : LP NP BP Sec

        Primary Path via    : 10.1.1.141, eth1
        FRR Backup Path via : 20.1.1.147, eth2
        FRR Metric          : 52
        Protection Provided : LP NP BP Sec

    R1#show ip route fast-reroute
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
    area ,p - stale info
           * - candidate default

    IP Route Table for VRF "default"
    i L1    40.1.1.0/24 [115/15] via 10.1.1.141, eth1, 00:17:34
                        [FRR-NH] via 20.1.1.147, eth2

    i L1    50.1.1.0/24 [115/15] via 10.1.1.143, eth1, 00:20:26
                        [FRR-NH] via 20.1.1.147, eth2

                       [115/15] via 30.1.1.148, eth3
                        [FRR-NH] via 10.1.1.141, eth1

    i L1    60.1.1.0/24 [115/5] via 30.1.1.148, eth3, 00:20:26
                        [FRR-NH] via 10.1.1.143, eth1

    i L1    70.1.1.0/24 [115/17] via 10.1.1.141, eth1, 00:17:34
                        [FRR-NH] via 30.1.1.148, eth3

    i L1    80.1.1.0/24 [115/35] via 10.1.1.141, eth1, 00:17:34
                        [FRR-NH] via 20.1.1.147, eth2

    i L1    90.1.1.0/24 [115/17] via 10.1.1.143, eth1, 00:20:26
                        [FRR-NH] via 20.1.1.147, eth2

                       [115/17] via 30.1.1.148, eth3
                        [FRR-NH] via 10.1.1.141, eth1

    i L1    146.146.146.146/32 [115/27] via 10.1.1.141, eth1, 00:06:19
                               [FRR-NH] via 20.1.1.147, eth2

                              [115/27] via 10.1.1.143, eth1
                               [FRR-NH] via 20.1.1.147, eth2
```



```
[115/27] via 30.1.1.148, eth3
 [FRR-NH] via 20.1.1.147, eth2
```

CHAPTER 7 IS-IS IPv6 Configuration

This chapter contains basic IS-IS (Intermediate System to Intermediate System) on IPv6 configuration examples.

Enable IS-ISv6 on an Interface

This example shows the minimum configuration required for enabling IS-IS on IPv6 on an interface. R1 and R2 are two routers in the ABC instance connecting to the network 1000::/64. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

Note: ISISv6 session will come up even if IPv6 address is not configured, as it will use the link local address present on the interfaces.

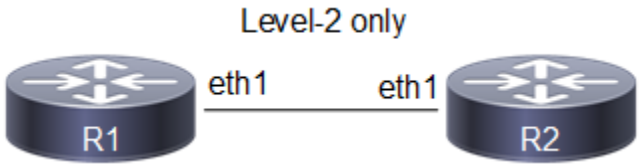


Figure 7-43: Figure 4-46: Basic IS-IS v6 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.

(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     27        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     7         L2   IS-IS
R2#

R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R1#

R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R2#

R1#
R1#show ipv6 isis topology
```

```
Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1        b86a.97c4.31c5

R1#

R2#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1        b86a.97cb.3ec5
0000.0000.0002       --
```

Set Priority

This example describes how to set the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R3 is configured to have a priority of 70, this is higher than the default priority (64) of R1 and R2. This makes R3 the DIS.

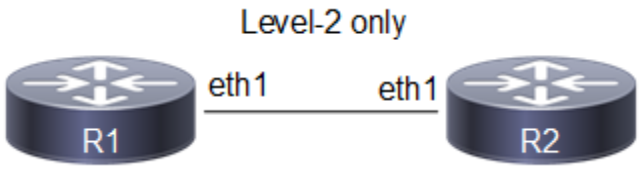


Figure 7-44: Set IS-IS Priority

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#isis priority 125`	Specify the router priority to a higher priority (125) to make R2 the designated IS (DIS).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     8         L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     26        L2   IS-IS
R2#


R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   125       0000.0000.0002.01
R1#

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```

```
0000.0000.0001 eth1        Up     L2   64         0000.0000.0002.01
R2#


R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00002722
    Local SNPA: b86a.97cb.3ec5
    IP interface address:
    IPv6 interface address:
      1000::1/64
      fe80::ba6a:97ff:fecb:3ec5/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds
R1#

R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00002722
    Local SNPA: b86a.97c4.31c5
    IP interface address:
    IPv6 interface address:
      1000::2/64
      fe80::ba6a:97ff:fec4:31c5/64
    Level-2 Metric: 10/10, Priority: 125, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 1 seconds
R2#
```

Dynamic hostname

This example shows how to configure Dynamic Hostname for an ISIS IPv6 instance. Dynamic hostname is the method of mapping name-to-systemID. It allows the routing protocol to advertise symbolic names in the IS-IS PDUs. This is done by the addition of a new TLV which allows the IS-IS routers to include the name-to-systemID mapping data in their LSPs. This allows for simple and reliable transport of name mapping across IS-IS networks.

Dynamic hostname can be either the hostname of the node or the tag of the configured ISISv6 instance.

Note: Dynamic-hostname has to be configured on all nodes for it to take effect.

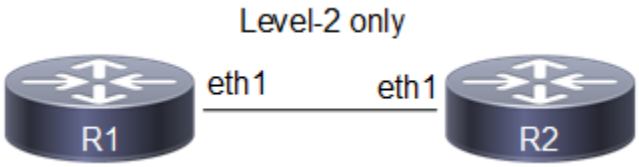


Figure 7-45: Basic dynamic hostname topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#end`	Exit the current mode and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#end`	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
```

```
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        b86a.97c4.31c5  Up     20        L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        b86a.97cb.3ec5  Up     8         L2   IS-IS
R2#



R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000008   0xFB86        1144              0/0/0
R1.01-00            * 0x00000005   0x19BD        1141              0/0/0
R2.00-00              0x00000007   0x245C        1140              0/0/0

R1#

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000008   0xFB86        1144              0/0/0
R1.01-00              0x00000005   0x19BD        1140              0/0/0
R2.00-00            * 0x00000007   0x245C        1140              0/0/0
R2.01-00            * 0x00000002   0xE710        0 (1132)          0/0/0

R2#



R1#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        b86a.97c4.31c5

R1#
```

```
R2#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        b86a.97cb.3ec5
R2                   --

R2#
```

Redistribute Routes into IS-IS

In this example, the configuration causes OSPFv3 routes to be imported into the IS-ISv6 routing table, and advertised into the ABC instance.

Topology

Figure 7-46: Redistribute Routes into IS-IS

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.

(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface and assign the Area ID 0.
(config-if)#ipv6 address 2000::1/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration
(config-router-af)#redistribute ospf	Enable redistribution of routes from ospf into the ISIS routing table.
(config-router-af)# exit-address-family	Exit address family mode.
(config-router)#exit	Exit router mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 2.2.2.2	Specify a Router ID (2.2.2.2) for the OSPFv3 routing process.
(config-router)#end	Exit the current mode and enter privilege mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface and assign the Area ID 0.
(config-if)#ipv6 address 2000::2/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 3.3.3.3	Specify a Router ID (3.3.3.3) for the OSPFv3 routing process.
(config-router)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     27        L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
```

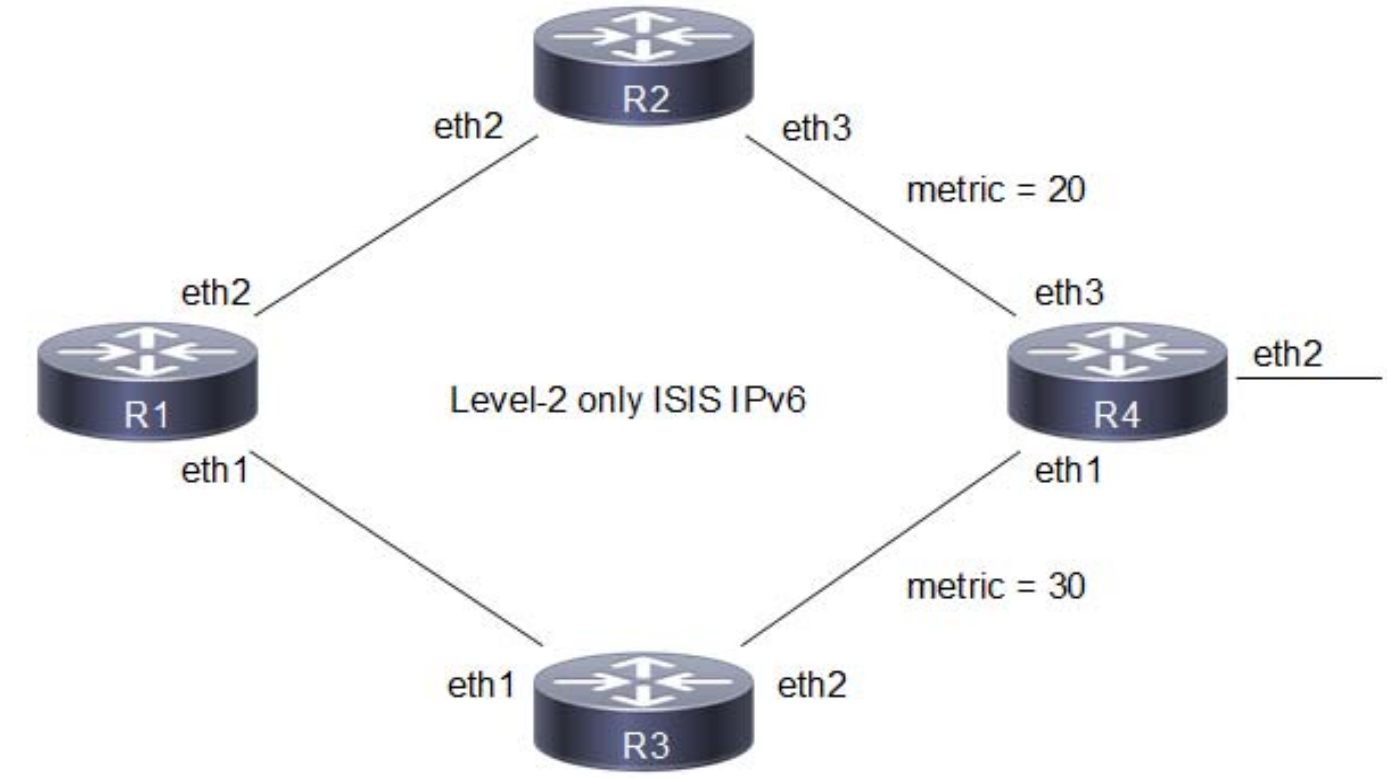
```
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     8         L2   IS-IS
R2#

R2#show ipv6 ospf neighbor

Total number of full neighbors: 1
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
3.3.3.3           1   Full/DR         00:00:34    eth2        0
R2#


R1#show ipv6 route isis
IP Route Table for VRF "default"
i L2   2000::/64 [115/10] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:21:19
R1#


R1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:33:07
C      1000::/64 via ::, eth1, 01:13:36
i L2   2000::/64 [115/10] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:21:29
C      fe80::/64 via ::, xe8, 00:39:44
R1#
```

Interface Metric

You can make a route the preferred route by changing its metric. In this example, the cost has been configured to make R3 the next hop for R1.

The default metric for each interface is 10. Interface eth2 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 9999::/64 (R4) through R2 and R3 is computed as follows: R2: 10+20 = 30 R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 9999::/64.



gy

Figure 7-47: Configure IS-IS Metric

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0100.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#end`	Exit current mode and enter privilege mode.

R2

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).

(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 20	Set the value of IS-IS metric (on eth2) to 20.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0100.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 30	Set the value of IS-IS metric (on eth2) to 30.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0100.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 address 9999::1/64	Configure ipv6 address in eth2
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0100.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#address-family ipv6	Enter ipv6 address family.
(config-router-af)#redistribute connected	Enable redistribution of connected routes into ISIS process
(config-router-af)#end	Exit current mode and enter privilege mode

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        b86a.97c4.31c5      Up     25        L2   IS-IS
0000.0000.0003 eth1         b86a.97c9.3cc5      Up     26        L2   IS-IS
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth3         b86a.97c7.32c5      Up     7         L2   IS-IS
0000.0000.0001 eth2        b86a.97cb.3ec5      Up     6         L2   IS-IS
R2#

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth2        b86a.97c7.32c5      Up     22        L2   IS-IS
0000.0000.0001 eth1         b86a.97cb.3ec5      Up     7         L2   IS-IS
R3#

R4#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth3         b86a.97c4.31c5      Up     22        L2   IS-IS
0000.0000.0003 eth1        b86a.97c9.3cc5      Up     7         L2   IS-IS
R4#


R1#show ipv6 isis route
```

```
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
L2   9999::/64 [30]
      via fe80::ba6a:97ff:fec4:31c5, eth2

R1#
```

Route Summarization

Route summarization makes the routing table smaller, but still allows complete IP connectivity.

The following example consists of a three-router topology, in which R2 is doing the summarization. In this example, R1 is the L1 router, R2 is the L1/L2 router doing the summarization, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacencies with R1 and R3 are already up, and the route tables with the appropriate routes are already populated.

Topology

Figure 7-48: Route Summarization Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)# is-type level-1`	Configure instance as level-1 routing.
`(config-router)#net 49.0001.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.

(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#isis circuit-type level-1	Set the circuit type as level-1 for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#isis circuit-type level-2-only	Set the circuit type as level-2-only for the interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#net 49.0001.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.
(config-router-af)#redistribute isis level-2 into level-1	Enable redistribution of isis routes from level-2 into level-1
(config-router-af)#summary-prefix 11:1:1:1::/64 level-1 metric 58	Configure the summary prefix to summarize IPv6 reachability information.
(config-router-af)#exit-address-family	Exit address family mode.
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#ipv6 route 11:1:1:1:1:1::/96 eth2	Configure ipv6 static route.
(config)#ipv6 route 11:1:1:1:2:1::/96 eth2	Configure ipv6 static route.
(config)#ipv6 route 11:1:1:1:3:1::/96 eth2	Configure ipv6 static route.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#isis circuit-type level-2-only	Set the circuit type as level-2-only for the interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#net 49.0001.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)# is-type level-2-only	Configure instance as level-2 -onlyrouting.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.
(config-router-af)#redistribute static	Enable redistribution of static routes into ISIS instance.
(config-router-af)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
```

```
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     21        L1   IS-IS
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2         b86a.97c7.32c5      Up     8         L2   IS-IS
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     8         L1   IS-IS
R2#


R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2         b86a.97c4.31c5      Up     20        L2   IS-IS
R3#



R1#show ipv6 route isis
IP Route Table for VRF "default"
i ia   11:1:1:1::/64 [115/68] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:02:29
R1#

R2#show ipv6 route isis
IP Route Table for VRF "default"
i      11:1:1:1::/64 [115/0] via ::, Null, 00:02:30
i L2   11:1:1:1:1:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
i L2   11:1:1:1:2:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
i L2   11:1:1:1:3:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
R2#

R3#show ipv6 route isis
IP Route Table for VRF "default"
R3#
```

```
R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
ia   11:1:1:1::/64 [68]
      via fe80::ba6a:97ff:fec4:31c5, eth1

R1#


R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
D    11:1:1:1::/64 [0]
      via ::
L2   11:1:1:1:1:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2
L2   11:1:1:1:2:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2
L2   11:1:1:1:3:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2

R2#


R3#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
E    11:1:1:1:1:1::/96 [0]
      via ::
E    11:1:1:1:2:1::/96 [0]
      via ::
E    11:1:1:1:3:1::/96 [0]
      via ::

R3#



R1#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
```

```
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000002   0xA557        497               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
0000.0000.0001.01-00* 0x00000001   0x1FBD        497               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000004   0x4DA0        909               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   58         IPv6-Interarea 11:1:1:1::/64

R1#


R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0xA557        496               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
0000.0000.0001.01-00  0x00000001   0x1FBD        496               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000004   0x4DA0        910               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   58         IPv6-Interarea 11:1:1:1::/64

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000002   0xCD2A        506               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0003.01
0000.0000.0003.00-00  0x00000003   0x89E2        765               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 11:1:1:1:1:1::/96
  Metric:   0          IPv6 11:1:1:1:2:1::/96
  Metric:   0          IPv6 11:1:1:1:3:1::/96
0000.0000.0003.01-00  0x00000001   0x2DA9        505               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00
```

R2#

Passive Interface

In ISP and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the Default Passive-Interface feature, there were two possibilities for obtaining routing information from tall of these interfaces:

- Configure a routing protocol on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive, which was time consuming.

The solution to this problem was to configure the routing protocol on all interfaces and manually set the passive interface command on the interfaces where adjacency was not desired. In certain networks, this meant coding 200 or more passive-interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single passive-interface default command, then configuring individual interfaces in which adjacencies are desired using the no passive-interface command.

Usage

1. When a specific interface is configured as passive using the passive-interface command:
   - The interface loses its adjacency on that interface, for example, eth1.
   - The interface (eth1) is still advertised by other IS-IS speaking interfaces to their neighbors.
2. When a specific interface is configured as passive using passive-interface command followed by removing the configuration using no passive-interface command:
   - The interface is IS-IS disabled and must be enabled using the ipv6 router isis command (for example, ipv6 router isis 1).
   - The interface (for example, eth1) is not advertised by other IS-IS speaking interfaces to their neighbors.
3. When an interface is configured with the passive interface command:
   - All interfaces lose their adjacency, except the interface with the higher index number. (For example: If eth1, eth2, eth3, and eth4 are the router interfaces, eth4 has the highest index number.)
   - All interfaces are advertised by the active IS-IS speaking interface to its neighbors.
4. When an interface is configured with the no passive interface command:
   - All interfaces are IS-IS disabled, except the interface that was active, and all interfaces must enable IS-IS on these interfaces using the ipv6 router isis command (for example, ipv6 router isis 1).
   - All interfaces are not advertised by the active IS-IS speaking interface to its neighbors.

Topology

Figure 7-49: IS-ISv6 Passive Interface

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#end`	Exit the current mode and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)# ipv6 router isis ABC`	Enable OSPFv3 routing on an interface and assign the Area ID 0.
`(config-if)#ipv6 address 2000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#passive-interface eth1`	Configure interface eth1 as a passive-interface.
`(config-router)#end`	Exit the current mode and enter privilege mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#ipv6 address 2000::2/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2         b86a.97c7.32c5      Up     7         L2   IS-IS
R2#


R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2         b86a.97c4.31c5      Up     24        L2   IS-IS
R3#


R1#show ipv6 isis route
```

```
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R1#


R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [0]
      via ::, eth1
C    2000::/64 [10]
      via ::, eth2

R2#

R3#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
L2   1000::/64 [10]
      via fe80::ba6a:97ff:fec4:31c5, eth2
C    2000::/64 [10]
      via ::, eth2

R3#


R1#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x0000000E   0x0E19        931               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::1
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00* 0x00000009   0xE110        0 (931)           0/0/0
0000.0000.0002.00-00  0x00000011   0xABC7        440               0/0/0
  Area Address: 49.0005
```

```
  NLPID:        0x8E
  IPv6 Address: 1000::2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00  0x00000002   0x9ED3        439               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
0000.0000.0003.01-00  0x00000001   0x2DA9        436               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R1#
R1#

R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000D   0x2666        879               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00  0x00000009   0x11C1        821               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000012   0x669F        906               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00  0x00000002   0x9ED3        439               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
0000.0000.0003.01-00  0x00000001   0x2DA9        436               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R2#
```

```
R3#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000D   0x2666        879               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00  0x00000009   0x11C1        821               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000012   0x669F        905               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00* 0x00000002   0x9ED3        440               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
0000.0000.0003.01-00* 0x00000001   0x2DA9        437               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R3#
```

Enable BFD over IS-ISv6

This example shows how to configure Bidirectional Forwarding Detection with ISISv6 instance

Topology

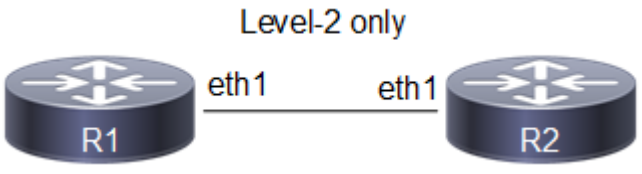


Figure 7-50: Basic BFD over IS-ISv6 Topology

Configuration

R1

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.
(config-router)#end	Exit current mode and enter privilege mode.

R2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.
(config-router)#end	Exit current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5  Up     24        L2   IS-IS
R1#

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
======================================================================================
```

```
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
256       256         IPv6        Single-Hop  Up         00:04:26  eth1         NA
fe80::ba6a:97ff:fec4:31c5/128
Number of Sessions:    1
R1#
R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10018          Interface name :eth1
Session Index : 256
Lower Layer : IPv6                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 256                Local Address : fe80::ba6a:97ff:fecb:3ec5/128
Remote Discriminator : 256               Remote Address : fe80::ba6a:97ff:fec4:31c5/128
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                                Pkt Out : n/a
Pkts Drop : 00000000000000000000            Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000             IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000001231          IPv6 Pkt Out : 00000000000000001233
UP Count : 1                                UPTIME : 00:04:30

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
R1#
```

Originate Default Route to ISISv6 Neighbors

This example shows how to originate default route present to ISISv6 neighbors.

Note: To get a default route in ISIS, we must have it (said default route) in the routing table first.

Topology

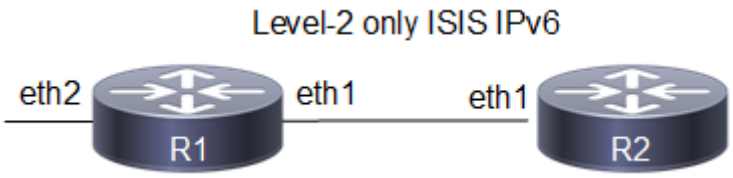


Figure 7-51: Basic IS-ISv6 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#ipv6 route ::/0 2345::2`	Configure default route.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 2345::1/64`	Configure IPv6 address on interface.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)# address-family ipv6`	Enter ipv6 address family.
`(config-router-af)#default-information originate`	Originate reachability information to Default destination into LSP.
`(config-router-af)#end`	Exit all modes and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#end`	Exit current mode and enter privilege mode

Validation

```
R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     6         L2   IS-IS
R2#

R2#show ipv6 route isis
IP Route Table for VRF "default"
i L2   ::/0 [115/10] via fe80::ba6a:97ff:fecb:3ec5, eth1, 00:09:12
R2#

R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
L2   ::/0 [10]
      via fe80::ba6a:97ff:fecb:3ec5, eth1

R2#
R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000006   0x5FA4        1033              0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   0          IPv6 ::/0
0000.0000.0001.01-00  0x00000001   0x21B9        628               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS R2.00
R2.00-00            * 0x00000002   0xFBED        633               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Hostname:     R2
  Metric:   10         IS 0000.0000.0001.01
```

CHAPTER 8 IS-IS-TE IPv4

This chapter contains basic IS-IS TE configuration examples.

For details about the commands used in these examples, see the *Intermediate System to Intermediate System Command Reference*.

A TE link represents an IS-IS/OSPF link state advertisement and a link state database of certain physical resources and their properties between two GMPLS nodes. Typically, a TE link is advertised as an adjunct to a “regular” OSPF or IS-IS link. That is, an adjacency is brought up on the link. When the link is up, both the regular IGP properties of the link (for example, the SPF metric) and the TE properties of the link are then advertised.

Enable MPLS-TE in Level-1 and Level-2 on L1-L2 IS

In the following example, R1 is the L1 router, R2 is the L1/L2 router enabling MPLS-TE for both Level-1 and Level-2 IS, and R3 is the L2 router. The following configuration is given for R1, R2 and R3.

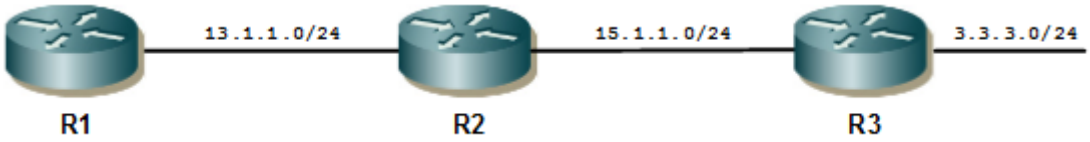


Figure 8-52: MPLS-TE Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 13.1.1.2/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#interface eth2`	Enter Interface eth2 configure mode.
`(config-if)#ip address 15.1.1.2/24`	Configure ip address to the interface eth2.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth2.
`(config-if)#isis circuit-type level-2`	Configure ISIS circuit-type as Level-2.
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#mpls traffic-eng router-id 2.2.2.2`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE in is-type Level-1.
`(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE in is-type Level-2.

`(config-router)#net 49.0001.0000.0000.0002.00`	Configure the ISIS net address with area id as: 49.0001 and system id as: 0000.0000.0002.
`(config-router)#end`	Exit Router mode.

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (eth1) to configure, and enter Interface mode.
`(config-if)#ip address 13.1.1.2/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#is-type level-1`	Configure IS-Type as Level-1 router.
`(config-router)#mpls traffic-eng router-id 1.1.1.1`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE in is-type Level-1.
`(config-router)#net 49.0001.0000.0000.0001.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0001.
`(config-router)#end`	Exit Router mode.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ip address 15.1.1.3/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-2`	Configure ISIS circuit-type as Level-2
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#is-type level-2`	Configure IS-Type as Level-1 router.
`(config-router)#mpls traffic-eng router-id 3.3.3.3`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE in is-type Level-2.
`(config-router)#net 49.0001.0000.0000.0003.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0003.
`(config-router)#end`	Exit Router mode.

Validation

R2

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors
Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.00bb.5e85  Up     24        L1   IS-IS
0000.0000.0003 eth4        5254.00ac.f960  Up     9         L2   IS-IS
#
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have correct router-id.

```
#sh isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000C   0x3129        1055              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.03
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 12500000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00* 0x00000014   0x3CE9        1192              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.03
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 12500000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0002.03-00* 0x00000005   0x685B        1028              0/0/0
  Metric:   0          IS-Extended 0000.0000.0002.00
  Metric:   0          IS-Extended 0000.0000.0001.00

#
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have correct router-id.

```
#sh isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x0000000F   0x8C9B        939               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.2
```

```
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 12500000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00  0x0000000C   0x8470        1193              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.3
    Maximum Link Bandwidth: 125000000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.01-00  0x00000004   0x8D36        1015              0/0/0
  Metric:   0          IS-Extended 0000.0000.0003.00
  Metric:   0          IS-Extended 0000.0000.0002.00
#
```

R1

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors

Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.00f6.4ae7  Up     7         L1   IS-IS
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have correct router-id.

```
#show isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x0000000C   0x3129        877               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.03
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 12500000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00  0x00000014   0x3CE9        1014              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.03
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 12500000.00
```

```
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0002.03-00  0x00000005   0x685B        851               0/0/0
  Metric:   0          IS-Extended 0000.0000.0002.00
  Metric:   0          IS-Extended 0000.0000.0001.00
#
```

R3

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#sh clns  neighbors

Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.0062.3ea6  Up     21        L2   IS-IS
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have correct router-id.

```
#show isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x0000000F   0x8C9B        819               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 12500000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00* 0x0000000C   0x8470        1073              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.3
    Maximum Link Bandwidth: 125000000.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.01-00* 0x00000004   0x8D36        895               0/0/0
  Metric:   0          IS-Extended 0000.0000.0003.00
  Metric:   0          IS-Extended 0000.0000.0002.00
#
```

Maximum Link Bandwidth and Reservable Bandwidth

In the following example, R1 is the L1 router, R2 is the L1/L2 router enabling MPLS-TE for both Level-1 and Level-2 IS, and R3 is the L2 router. The following configuration is given for R1, R2 & R3.

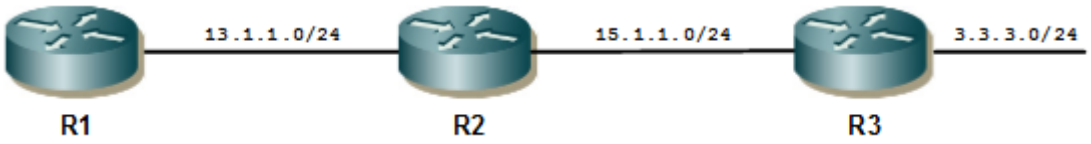


Figure 8-53: MPLS-TE Topology

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 13.1.1.2/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#interface eth2`	Enter Interface eth2 configure mode.
`(config-if)#ip address 15.1.1.2/24`	Configure ip address to the interface eth2.
`(config-if)#`	ip router isis 1Enable ISIS on interface eth2.
`(config-if)#isis circuit-type level-2`	Configure ISIS circuit-type as Level-2.
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#mpls traffic-eng router-id 2.2.2.2`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE in is-type Level-1.
`(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE in is-type Level-2.
`(config-router)#net 49.0001.0000.0000.0002.00`	Configure the ISIS net address with area id as: 49.0001 and system id as: 0000.0000.0002.
`(config-router)#exit`	Exit Router mode.
`(config)#interface eth2`	Enter the interface configure mode.
`(config-if)#bandwidth 1g`	Configure Maximum link Bandwidth as 1g bits per second.
`(config-if)#reservable-bandwidth 100m`	Specify the maximum reservable bandwidth per interface.
`(config-if)#exit`	Exit interface configure mode.
`(config)#interface eth4`	Enter the interface configure mode.
`(config-if)#bandwidth 500m`	Configure Maximum link Bandwidth as 500m bits per second.
`(config-if)#reservable-bandwidth 200m`	Specify the maximum reservable bandwidth per interface.
`(config-if)#`	Exit interface configure mode.

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 13.1.1.2/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#is-type level-1`	Configure IS-Type as Level-1 router.
`(config-router)#mpls traffic-eng router-id 1.1.1.1`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE in is-type Level-1.
`(config-router)#net 49.0001.0000.0000.0001.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0001.
`(config-router)#exit`	Exit Router mode.
`(config)#interface eth1`	Enter the interface configure mode.
`(config-if)#bandwidth 1g`	Configure Maximum link Bandwidth as 1g bits per second.
`(config-if)#reservable-bandwidth 100m`	Specify the maximum reservable bandwidth per interface.
`(config-if)#exit`	Exit interface configure mode.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ip address 15.1.1.3/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#exit`	Exit from interface configuration mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#is-type level-2`	Configure IS-Type as Level-2 router.
`(config-router)#mpls traffic-eng router-id 3.3.3.3`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE in is-type Level-2.
`(config-router)#net 49.0001.0000.0000.0003.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0003.
`(config-router)#exit`	Exit Router mode.
`(config)#interface eth1`	Enter the interface configure mode.

(config-if)#bandwidth 1g	Configure Maximum link Bandwidth as 1g bits per second.
(config-if)#reservable-bandwidth 100m	Specify the maximum reservable bandwidth per interface.
(config-if)#exit	Exit interface configure mode.

Validation

R2

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

#show clns neighbors

```
Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.00bb.5e85  Up     23        L1   IS-IS
0000.0000.0003 eth4        5254.00ac.f960  Up     9         L2   IS-IS
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have configured Max Link Bandwidth and Reservable Bandwidth.

```
#show isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000009   0x53C9        554               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.01
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00* 0x0000000B   0x36A2        1185              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.01
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
```

```
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0002.01-00* 0x00000007   0x7251        825               0/0/0
  Metric:   0          IS-Extended 0000.0000.0002.00
  Metric:   0          IS-Extended 0000.0000.0001.00
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have configured Max Link Bandwidth and Reservable Bandwidth.

```
#show isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x0000000B   0xA332        1160              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00  0x0000000B   0xA65F        1099              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.3
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
```

```
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.01-00  0x00000007   0x8739        795               0/0/0
  Metric:   0          IS-Extended 0000.0000.0003.00
  Metric:   0          IS-Extended 0000.0000.0002.00

#
```

R1

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors

Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.00f6.4ae7  Up     9         L1   IS-IS
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have configured Max Link Bandwidth and Reservable Bandwidth.

```
#show isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000009   0x53C9        392               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.01
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00  0x0000000B   0x36A2        1023              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.01
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
```



```
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0002.01-00  0x00000007   0x7251        663               0/0/0
  Metric:   0          IS-Extended 0000.0000.0002.00
  Metric:   0          IS-Extended 0000.0000.0001.00

#
```

R3

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors

Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.0062.3ea6  Up     26        L2   IS-IS
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have configured Max Link Bandwidth and Reservable Bandwidth.

```
#show isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x0000000B   0xA332        1068              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00* 0x0000000B   0xA65F        1007              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
```

```
      IPv4 Interface Address: 15.1.1.3
      Maximum Link Bandwidth: 62500000.00
      Reservable Bandwidth: 25000000.00
      Unreserved Bandwidth:
        Unreserved Bandwidth at priority 0: 0.00
        Unreserved Bandwidth at priority 1: 0.00
        Unreserved Bandwidth at priority 2: 0.00
        Unreserved Bandwidth at priority 3: 0.00
        Unreserved Bandwidth at priority 4: 0.00
        Unreserved Bandwidth at priority 5: 0.00
        Unreserved Bandwidth at priority 6: 0.00
        Unreserved Bandwidth at priority 7: 0.00
      TE-Default Metric: 1
    Metric:   10         IP-Extended 15.1.1.0/24
  0000.0000.0003.01-00* 0x00000007   0x8739        703               0/0/0
    Metric:   0          IS-Extended 0000.0000.0003.00
    Metric:   0          IS-Extended 0000.0000.0002.00

  #
```

Administrative Group Constraints

To configure administrative group constraints (also known as color constraints) in Level-1 and Level-2 on L1-L2 IS:

- Configure support for required admin groups in NSM on all participating routers
- Configure required administrative groups on all participating interfaces

The configuration in this example forces the primary LSP to be setup through links that belong either to admin group A or C. A link that does not belong to either of these admin groups will not be used for setting up the LSP.

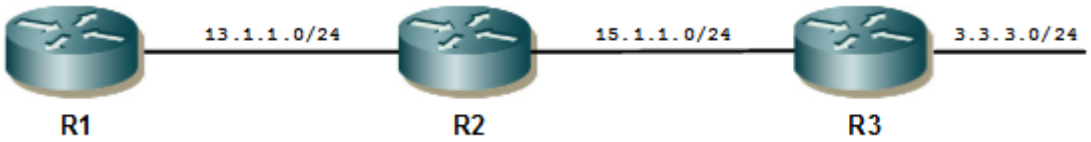


Figure 8-54: MPLS-TE Topology

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 13.1.1.2/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config)#interface eth2`	Enter Interface eth2 configure mode.
`(config-if)#ip address 15.1.1.2/24`	Configure ip address to the interface eth2.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth2.
`(config-if)#isis circuit-type level-2`	Configure ISIS circuit-type as Level-2.
`(config-if)#exit`	Exit from interface configuration mode.

(config)#mpls admin-group a 0	Add new administrative groups and specify their names and assign bit values to them.
(config)#mpls admin-group b 1	
(config)#mpls admin-group c 2	
(config)#mpls admin-group d 3	
(config)#router isis 1	Create an IS-IS routing instance for area 49 (1).
(config-router)#metric-style wide	Configure the new style of metric type as wide.
(config-router)#mpls traffic-eng router-id 2.2.2.2	Configure MPLS-TE unique router-id TLV.
(config-router)#mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1.
(config-router)#mpls traffic-eng level-2	Enable MPLS-TE in is-type Level-2.
(config-router)#net 49.0001.0000.0000.0002.00	Configure the ISIS net address with area id as: 49.0001 and system id as: 0000.0000.0002.
(config-router)#exit	Exit Router mode.
(config)#interface eth2	Enter the interface configure mode.
(config-if)#admin-group a	Add administrative groups to the links. When used in the interface mode, this command adds a link between an Interface and a group. The name is the name of the group Previously configured. You can have multiple groups per Interface.
(config-if)#admin-group c	
(config-if)#exit	Exit interface configure mode.
(config)#interface eth4	Enter the interface configure mode.
(config-if)#admin-group b	Add administrative groups to the links. When used in the interface mode, this command adds a link between an Interface and a group. The name is the name of the group previously configured. You can have multiple groups per Interface.
(config-if)#admin-group d	
(config-if)#end	Exit interface configure mode.

R1

#configure terminal	Enter Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip address 13.1.1.2/24	Configure ip address to the interface eth1.
(config-if)#ip router isis 1	Enable ISIS on interface eth1.
(config-if)#isis circuit-type level-1	Configure ISIS circuit-type as Level-1
(config-if)#exit	Exit interface configure mode.
(config)#mpls admin-group a 0	Add new administrative groups and specify their names and assign bit values to them.
(config)#mpls admin-group c 2	
(config)#router isis 1	Create an IS-IS routing instance for area 49 (1).
(config-router)#metric-style wide	Configure the new style of metric type as wide.
(config-router)#is-type level-1	Configure IS-Type as Level-1 router.
(config-router)#mpls traffic-eng router-id 1.1.1.1	Configure MPLS-TE unique router-id TLV.

`(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE in is-type Level-1.
`(config-router)#net 49.0001.0000.0000.0001.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0001.
`(config-router)#exit`	Exit Router mode.
`(config)#interface eth1`	Enter the interface configure mode.
`(config-if)#admin-group a`	Add administrative groups to the links. When used in the interface mode, this command adds a link between an Interface and a group. The name is the name of the group Previously configured. You can have multiple groups per Interface.
`(config-if)#admin-group c`	
`(config-if)#end`	Exit interface configure mode.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ip address 15.1.1.3/24`	Configure ip address to the interface eth1.
`(config-if)#ip router isis 1`	Enable ISIS on interface eth1.
`(config-if)#isis circuit-type level-1`	Configure ISIS circuit-type as Level-1
`(config-if)#exit`	Exit interface configure mode.
`(config)#mpls admin-group b 1`	Add new administrative groups and specify their names and assign bit values to them.
`(config)#mpls admin-group d 3`	
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 (1).
`(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`(config-router)#is-type level-2`	Configure IS-Type as Level-2 router.
`(config-router)#mpls traffic-eng router-id 3.3.3.3`	Configure MPLS-TE unique router-id TLV.
`(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE in is-type Level-2.
`(config-router)#net 49.0001.0000.0000.0003.00`	Configure the ISIS net address with area id as: 49.0001 and system-id as: 0000.0000.0003.
`(config-router)#exit`	Exit Router mode.
`(config)#interface eth1`	Enter the interface configure mode.
`(config-if)#admin-group b`	Add administrative groups to the links. When used in the interface mode, this command adds a link between an Interface and a group. The name is the name of the group Previously configured. You can have multiple groups per Interface.
`(config-if)#admin-group d`	
`(config-if)#end`	Exit interface configure mode.

Validation

R2

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors

Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.00bb.5e85      Up     24        L1   IS-IS
0000.0000.0003 eth4        5254.00ac.f960      Up     9         L2   IS-IS
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have configured admin-group constraints in Level-1.

```
#show isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000053   0x7B3F        1034              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.01
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00* 0x00000054   0xC9AD        595               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.01
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
```

```
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0002.01-00* 0x0000004F   0xE199        800               0/0/0
  Metric:   0          IS-Extended 0000.0000.0002.00
  Metric:   0          IS-Extended 0000.0000.0001.00
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have configured admin-group constraints in Level-2.

```
#show isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000054   0x115E        988               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    Admin-Group:
      Group 1
      Group 3
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00  0x00000054   0xC2DC        1079              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
    Admin-Group:
      Group 1
      Group 3
    IPv4 Interface Address: 15.1.1.3
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
```

```
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.01-00  0x0000004F   0xF681        788               0/0/0
  Metric:   0          IS-Extended 0000.0000.0003.00
  Metric:   0          IS-Extended 0000.0000.0002.00

#
```

R1

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors
Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.00f6.4ae7  Up     7         L1   IS-IS
```

Check the output of “show isis database level-1 verbose” to verify that LSP does have configured admin-group constraints in Level-1.

```
#show isis database level-1 verbose
Area 1:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000053   0x7B3F        1089              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.1
  Router ID:    1.1.1.1
  Metric:   10         IS-Extended 0000.0000.0002.01
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.1
    Maximum Link Bandwidth: 125000000.00
    Reservable Bandwidth: 12500000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
0000.0000.0002.00-00  0x00000054   0xC9AD        650               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0002.01
    Admin-Group:
      Group 0
      Group 2
    IPv4 Interface Address: 13.1.1.2
    Maximum Link Bandwidth: 125000000.00
```

```
      Reservable Bandwidth: 12500000.00
      Unreserved Bandwidth:
        Unreserved Bandwidth at priority 0: 0.00
        Unreserved Bandwidth at priority 1: 0.00
        Unreserved Bandwidth at priority 2: 0.00
        Unreserved Bandwidth at priority 3: 0.00
        Unreserved Bandwidth at priority 4: 0.00
        Unreserved Bandwidth at priority 5: 0.00
        Unreserved Bandwidth at priority 6: 0.00
        Unreserved Bandwidth at priority 7: 0.00
      TE-Default Metric: 1
    Metric:   10         IP-Extended 13.1.1.0/24
    Metric:   10         IP-Extended 15.1.1.0/24
  0000.0000.0002.01-00  0x0000004F   0xE199        855              0/0/0
    Metric:   0          IS-Extended 0000.0000.0002.00
    Metric:   0          IS-Extended 0000.0000.0001.00
  #
```

R3

Check the output of “show clns neighbors” to verify that ISIS adjacency is up.

```
#show clns neighbors
Area 1:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.0062.3ea6  Up     28        L2   IS-IS
```

Check the output of “show isis database level-2 verbose” to verify that LSP does have configured admin-group constraints in Level-2.

```
#show isis database level-2 verbose
Area 1:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000054   0x115E        1104              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   13.1.1.2
  Router ID:    2.2.2.2
  Metric:   10         IS-Extended 0000.0000.0003.01
    Admin-Group:
      Group 1
      Group 3
    IPv4 Interface Address: 15.1.1.2
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 13.1.1.0/24
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.00-00* 0x00000054   0xC2DC        1195              0/0/0
```

```
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   15.1.1.3
  Router ID:    3.3.3.3
  Metric:   10         IS-Extended 0000.0000.0003.01
    Admin-Group:
      Group 1
      Group 3
    IPv4 Interface Address: 15.1.1.3
    Maximum Link Bandwidth: 62500000.00
    Reservable Bandwidth: 25000000.00
    Unreserved Bandwidth:
      Unreserved Bandwidth at priority 0: 0.00
      Unreserved Bandwidth at priority 1: 0.00
      Unreserved Bandwidth at priority 2: 0.00
      Unreserved Bandwidth at priority 3: 0.00
      Unreserved Bandwidth at priority 4: 0.00
      Unreserved Bandwidth at priority 5: 0.00
      Unreserved Bandwidth at priority 6: 0.00
      Unreserved Bandwidth at priority 7: 0.00
    TE-Default Metric: 1
  Metric:   10         IP-Extended 15.1.1.0/24
0000.0000.0003.01-00* 0x0000004F   0xF681        904               0/0/0
  Metric:   0          IS-Extended 0000.0000.0003.00
  Metric:   0          IS-Extended 0000.0000.0002.00
```

CHAPTER 9 IS-IS Graceful Restart Configuration

The Intermediate System to Intermediate System (IS-IS) routing protocol is a link state intra-domain routing protocol. Normally, when an IS-IS router is restarted, temporary disruption of routing occurs due to events in both the restarting router and the neighbors of the restarting router.

ISIS provides graceful restart, in which the adjacency and routes are maintained in the routing table for the grace period. In this way, the data flow is not affected, and there is no packet loss during the restart phase.

With ISIS GR, the ISIS router should be able to restart gracefully with non-stop forwarding during the recovery. And the Helper ISIS router should be able to help restarting router by maintaining the adjacency.

ISIS Grace Restart Functionality applies to:

- ISIS broadcast network
- ISIS point-to-point network
- IPv4 domain
- IPv6 domain

Topology

In this example, R1 is the L1/L2 router, and R2 is the L1/L2 restart-helper router.

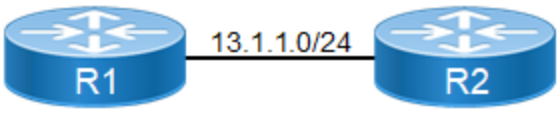


Figure 9-55: IS-IS Graceful Restart

Configuration

The following configuration is given only for R2, assuming that the adjacency with R1 is already up and the route tables with the appropriate routes are already populated.

R2

`#configure terminal`	Enter configure mode.
`(config)#isis restart helper`	Configure this router as a restart helper.
`(config)#isis restart grace-period 100`	Set the grace period to 100 seconds. The restarting router should come up before 100 seconds, otherwise, the adjacency and routes will be deleted.

Note: The IS-IS daemon in the restarting router must be manually restarted using `restart isis graceful` command: it does not restart automatically.

Note: The scope of unplanned GR is that if the ISIS daemon crashes or gets killed with SIGSEGV signal then the routes will be stale marked until the hold time (30 seconds), assuming that ISIS will be restarted within the hold time. Neighbor adjacency cannot be maintained in unplanned GR.

Validation

```
R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     13.1.1.0/24 is directly connected, eth1, 04:08:20
i ia  20.0.0.0/6 [115/11] via 13.1.1.2, eth1, 00:10:44
i L1  33.0.0.0/24 [115/20] via 13.1.1.2, eth1, 00:10:44
C     127.0.0.0/8 is directly connected, lo, 04:10:59
C     192.168.52.0/24 is directly connected, eth0, 04:10:55


R2#show clns neighbors

Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.0099.1e21      Up     20        L1   IS-IS


R2#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  13.1.1.0/24 is directly connected, eth1, 04:10:56
i L1     13.1.1.0/24 [115/10] is directly connected, eth1, 01:58:50
i ia *>  20.0.0.0/6 [115/11] via 13.1.1.2, eth1, 00:13:20
i L1 *>  33.0.0.0/24 [115/20] via 13.1.1.2, eth1, 00:13:20
C    *>  127.0.0.0/8 is directly connected, lo, 04:13:35
C    *>  192.168.52.0/24 is directly connected, eth0, 04:13:31

Gateway of last resort is not set
```

CHAPTER 10 Forwarding Plane Load Balancing

OcNOS uses Forwarding Plane Load Balancing when the kernel supports Equal Cost Multipath (ECMP). OcNOS installs the maximum number of ECMP routes supported by the kernel. This allows for load balancing to be performed with more than one nexthop to reach a destination. If the router receives and installs multiple paths with the same administrative distance and cost to a destination, load-balancing is possible.

Ideally, multiple nexthops have different interfaces to the destination, but this is not mandatory. The algorithm for distributing traffic across ECMP routes is dependent on the kernel, and typically based on the protocol, source address, destination address, and port.

Enable Load Balancing

The following example illustrates how to enable Equal Cost Multipath (ECMP), and configure a routing protocol (OSPF is used in this example) for load balancing. However, this example will not work if the kernel does not support load balancing. In this topology, R1, R2, and R3 are three Linux routers connected to each other. R1 can reach R3 through two links available to R2.

Topology

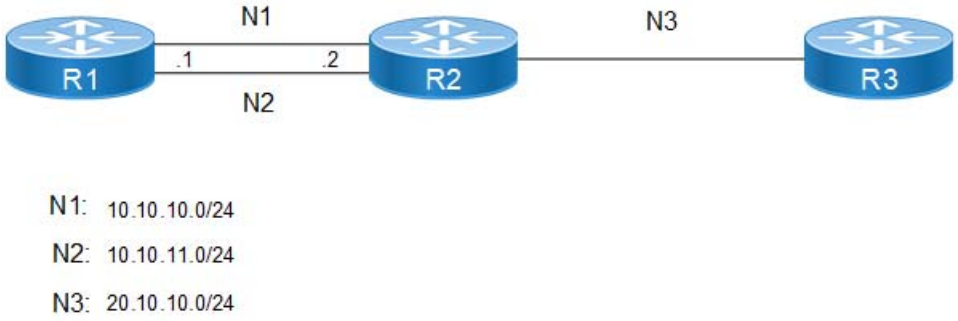


Figure 10-56: Load Balancing Topology

Configuration

R1 - NSM

1. Enable multipath support and set the maximum number of paths to be installed in the Forwarding Information Base (FIB):

```
#configure terminal
(config)#maximum-paths 2
% System Reboot is required for new Maximum-Path value to take effect.
```

Note: User can save and reboot to bring changes into effect.

R1 - OSPF

1. Configure OSPF on all interfaces on R1, R2, and R3.

   R1 learns about R3 through 2 nexthops (both networks N1 and N2).

Validation

R1 - OSPF

Run the `show ip ospf route` command on R1. The OSPF routing table displays that it can reach R3 through both of the nexthops:

```
R1#show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   C  10.10.10.0/24 [10] is directly connected, eth1, Area 0.0.0.0
   C  10.10.11.0/24 [10] is directly connected, eth2, Area 0.0.0.0
   O  20.10.10.0/24 [11] via 10.10.10.3, eth1, Area 0.0.0.0
                         via 10.10.11.3, eth2, Area 0.0.0.0
```

Run the `show ip route` command on R1. It displays that R1 has installed both nexthops to reach R3 in the NSM routing table:

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.10.10.0/24 is directly connected, eth1, 00:17:08
C     10.10.11.0/24 is directly connected, eth2, 00:16:49
O     20.10.10.0/24 [110/11] via 10.10.11.3, eth2, 00:08:52
             [110/11] via 10.10.10.3, eth1
C     127.0.0.0/8 is directly connected, lo, 00:25:21
C     192.168.52.0/24 is directly connected, eth0, 00:25:16

Gateway of last resort is not set
```

CHAPTER 11 VLAN Interfaces

This chapter contains examples for configuring VLAN interfaces.

Overview

Several Virtual LAN (VLAN) interfaces can be configured on a single Ethernet interface. Once created, a VLAN interface functions the same as any physical interface.

NSM recognizes VLAN interfaces as physical interfaces. Once VLAN interfaces are created in the kernel, and IP addresses are assigned to them, OcNOS commands can be used to configure and display VLAN interfaces the same as any physical interface. OcNOS routing protocols, such as OSPF and BGP can run across networks using VLAN interfaces.

Two systems with physical connectivity (either directly connected or connected through a switch), can communicate with each other via VLAN interfaces that have the same VLAN IDs and belong to the same network.

If the physical interfaces are not directly connected to a switch, the corresponding ports on the switch must be configured as trunks, and should not be associated to any VLANs in the switch. The commands to configure switch ports as trunks depend on the type of the switch, and are beyond the scope of this document.

Topology

Figure 11-57 is used to describe VLAN interface configuration. In this example, there are two routers, R1 and R2, and the eth1 interface of R1 is connected directly to eth2 using an ethernet cable.

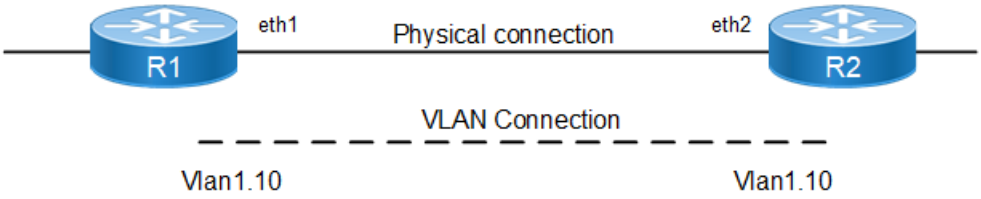


Figure 11-57: VLAN Connections

The `vlan1.10` VLAN interface is created on R1, and `vlan1.10` is created on R2. The VLAN interfaces are configured in the same network: R1 and R2 can reach each other using the VLAN connection.

Note: A VLAN ID of both VLAN interfaces is the same (10). Two systems with different VLAN IDs cannot communicate, even if they are in the same network, since a VLAN ID tags packets sent on a VLAN interface.

Create a VLAN Interface

When a VLAN interface is configured, a Layer 3 interface based on the bridge-group number and VLAN ID is created. This Layer 3 interface is advertised to all the Layer 3 protocols.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Create a MSTP bridge.
`(config)#vlan database`	Enter VLAN mode.
`(config-vlan)#vlan 10 bridge 1`	Enable VLAN 10 on bridge 1.
`(config-vlan)#exit`	Exit VLAN mode.

`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure interface as Layer2 interface.
`(config-if)#bridge-group 1`	Associate bridge group 1.
`(config-if)#switchport mode trunk`	Configure interface eth1 as Layer2 trunk mode.
`(config-if)#switchport trunk allowed vlan add 10`	Associate VLAN 10 as trunk port.
`(config-if)#exit`	Exit interface mode.

Add IP Addresses to VLAN Interface

In NSM, you can add or remove IP addresses from VLAN interfaces, like normal interfaces. Using IMISH type:

```
#configure terminal
(config)#interface vlan1.10
(config-if)#ip address 192.168.1.50/24
```

Display VLAN Interfaces

In OcNOS, VLAN interfaces appear as any physical interfaces, in the `show running-config` or the `show ip interface brief` outputs, and can be configured as any other interface.

The following is a sample output of the `show ip interface brief` command on R1.

Note: The IP address of interface `vlan1.10` has correctly been changed by NSM:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
eth0                 10.12.56.26     up                    up
lo                   127.0.0.1       up                    up
lo.management        127.0.0.1       up                    up
vlan1.1              unassigned      up                    up
vlan1.10             192.168.1.50    up                    up
xe1                  unassigned      up                    up
xe2                  unassigned      up                    up
xe3                  unassigned      up                    down
xe4                  unassigned      up                    down
xe5                  unassigned      up                    down
xe6                  unassigned      up                    down
xe7                  unassigned      up                    down
xe8                  unassigned      up                    down
xe9                  unassigned      up                    down
xe10                 unassigned      up                    down
xe11                 unassigned      up                    down
xe12                 unassigned      up                    down
xe13                 unassigned      up                    up
xe14                 unassigned      up                    down
xe15                 unassigned      up                    down
xe16                 unassigned      up                    up
xe17                 unassigned      up                    down
```

```
xe18                unassigned      up                  down
xe19                unassigned      up                  down
xe20                unassigned      up                  down
xe21                unassigned      up                  down
xe22                unassigned      up                  down
xe23                unassigned      up                  down
xe24                unassigned      up                  down
xe25                unassigned      up                  down
xe26                unassigned      up                  down
xe28                unassigned      up                  down
xe29                unassigned      up                  down
xe30                unassigned      up                  down
xe31                unassigned      up                  down
xe32                unassigned      up                  up
xe33                unassigned      up                  down
xe34                unassigned      up                  down
xe35                unassigned      up                  down
xe36                unassigned      up                  down
xe37                unassigned      up                  up
xe38                unassigned      up                  down
xe39                unassigned      up                  down
xe40                unassigned      up                  down
xe41                unassigned      up                  up
xe42                unassigned      up                  down
xe43                unassigned      up                  down
xe44                unassigned      up                  down
xe45                unassigned      up                  up
xe46                unassigned      up                  down
xe47                unassigned      up                  down
xe48                unassigned      up                  up
xe49/1              unassigned      up                  up
xe49/2              unassigned      up                  down
xe49/3              unassigned      up                  down
xe49/4              unassigned      up                  down
xe50/1              unassigned      up                  up
xe50/2              unassigned      up                  down
xe50/3              unassigned      up                  down
xe50/4              unassigned      up                  down
xe51/1              unassigned      up                  down
xe51/2              unassigned      up                  down
xe51/3              unassigned      up                  down
xe51/4              unassigned      up                  down
xe52/1              unassigned      up                  down
xe52/2              unassigned      up                  down
xe52/3              unassigned      up                  down
xe52/4              unassigned      up                  down
xe53/1              unassigned      up                  up
xe53/2              unassigned      up                  down
xe53/3              unassigned      up                  down
xe53/4              unassigned      up                  down
```

```
xe54/1              unassigned      up                  up
xe54/2              unassigned      up                  down
xe54/3              unassigned      up                  down
xe54/4              unassigned      up                  down
```

Below is the NSM routing table, which shows the connected network `192.168.1.0/24` of `vlan1.10`. These interfaces will now act as any physical interfaces, and all routing protocols will run across this network.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter+F27 area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     127.0.0.0/8 is directly connected, lo, 00:16:43
C     192.168.1.0/24 is directly connected, vlan1.10, 00:02:05
C     192.168.52.0/24 is directly connected, eth0, 00:16:39

Gateway of last resort is not set
```

CHAPTER 12 Layer 3 Link Aggregation

This chapter contains a complete sample Link Aggregation Control Protocol (LACP) configuration (L3 LAG).

Link Aggregation is the method of combining individual physical network interfaces or ports to increase the capacity of the link to support and sustain beyond the individual port capability. Features like Spanning Tree, VLAN, FDB, Multicast operate on both physical ports as well as Link Aggregated Logical Ports. It bundles all of the controller's distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption.

The OcNOS LACP implementation supports the aggregation of a maximum of six physical Ethernet links into a single logical channel.

Topology

In this example, 3 links are configured between the two switches R1 and R2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by STP as one interface.

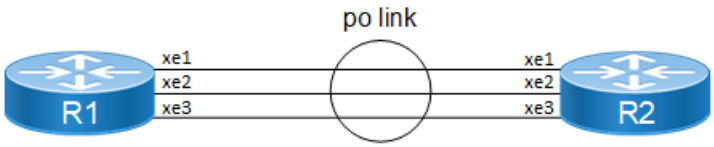


Figure 12-58: L3_LAG Topology

Configuration

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface po10`	Enter interface mode.
`R1(config-if)#ip address 1.1.1.1/24`	Assigning IP Address to PO Interface
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`R1(config)#interface xe1`	Enter interface mode.
`R1(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R1(config-if)#exit`	Exit interface mode.

`R1(config)#interface xe2`	Enter interface mode.
`R1(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface xe3`	Enter interface mode.
`R1(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R1(config-if)#exit`	Exit interface mode.

R2

`R2#configure terminal`	Enter configure mode.
`R1(config)#interface po10`	Enter interface mode.
`R1(config-if)#ip address 1.1.1.2/24`	Assigning IP Address to PO Interface
`R1(config-if)#exit`	Exit interface mode.
`R2(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`R2(config)#interface xe1`	Enter interface mode.
`R2(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Enter interface mode.
`R2(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe3`	Enter interface mode.
`R2(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`R2(config-if)#exit`	Exit interface mode.

Static Channel-group

R1

`R1#configure terminal`	Enter configure mode
`R1(config)#interface sa12`	Enter interface mode
`R1(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R1(config-if)#ip address 2.2.2.1/24`	Assigning IP Address to PO Interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe1`	Enter interface mode
`R1(config-if)#static-channel-group 12`	Add this interface to channel group 12 and enable link aggregation so that it can be selected for aggregation by the local system.
`R1(config-if)#exit`	Exit interface mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#interface sa12`	Enter interface mode
`R2(config-if)#no switchport`	Making Interface as L3 Port (This command will remove if switchport configuration is present).
`R2(config-if)#ip address 2.2.2.2/24`	Assigning IP Address to PO Interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#interface xe1`	Enter interface mode
`R2(config-if)#static-channel-group 12`	Add this interface to channel group 12 and enable link aggregation so that it can be selected for aggregation by the local system.
`R2(config-if)#exit`	Exit interface mode

Validation

show etherchannel detail, show etherchannel summary

```
#sh etherchannel summary
% Aggregator po10 100010
% Aggregator Type: Layer3
% Admin Key: 0010 - Oper Key 0010
%   Link: xe1 (10049) sync: 1
%   Link: xe2 (10050) sync: 1
%   Link: xe3 (10051) sync: 1

#sh etherchannel detail
% Aggregator po10 100010
% Aggregator Type: Layer3
%  Mac address: 14:18:77:5d:5c:01
%  Admin Key: 0010 - Oper Key 0010
```

```
%  Actor LAG ID- 0x4e20,14-18-77-01-5c-00,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,14-18-77-01-73-00,0x000a
%   Link: xe1 (10049) sync: 1
%   Link: xe2 (10050) sync: 1
%   Link: xe3 (10051) sync: 1
% Collector max delay: 5

#sh etherchannel 10
% Aggregator po10 100010 Admin Key: 0010 - Oper Key 0010
% Partner LAG ID: 0x4e20,14-18-77-01-73-00,0x000a
% Partner Oper Key 0010

#sh etherchannel
% Lacp Aggregator: po10
% Member:
   xe1
   xe2
   xe3
#show static-channel-group
%Static Aggregator: sa12
% Member Status
%   xe1    up
%   xe2    up
%   xe3    up
```

CHAPTER 13 Static Routes

This chapter contains basic static routing configuration examples.

This example shows the complete configuration to enable static routing in a simple network topology. A static route is composed of a network prefix (host address) and a nexthop (gateway). Static routes are useful in small networks. They are simple solutions for making a few destinations reachable. Large networks use dynamic routing protocols.

For details about the commands used in these examples, see the *Unicast Routing Information Base Command Reference*.

Topology

Router R1 is configured with these static routes:

- The remote network 10.10.12.0/24
- The loopback address (host addresses) of router R2
- The loopback address of router R3

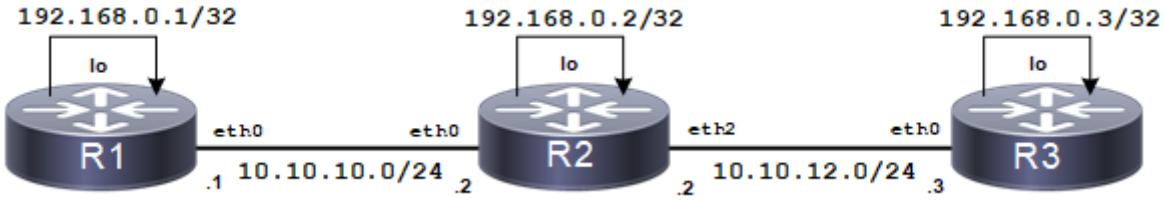


Figure 13-59: Basic Static Route

In all three routes, interface `eth0` of router R2 is the gateway. Router R3 is configured with a default static route that is equivalent to configuring separate static routes with the same gateway or nexthop address. Router R2 has two routes, one for each of the remote routers' loopback address.

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.1/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit interface mode.

`(config)#ip route 10.10.12.0/24 10.10.10.2`
`(config)#ip route 192.168.0.2/32 10.10.10.2`
`(config)#ip route 192.168.0.3/32 10.10.10.2`
	Specify the destination prefix and mask for the network and a gateway.
	Because R2 is the only next hop available, you can configure a default route instead of configuring the same static route for individual addresses. See the configuration of R3.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.2/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit Interface mode.
`(config)#ip route 192.168.0.1/32 10.10.10.1` `(config)#ip route 192.168.0.3/32 10.10.12.3`	Specify the destination and mask for the network and a gateway.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.3/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit Interface mode.
`(config)#ip route 0.0.0.0/0 10.10.12.2`	Specify 10.10.12.2 as a default gateway to reach any network. Because 10.10.12.2 is the only available route, you can specify it as the default gateway instead of specifying it as the gateway for an individual network or host address.

Validation

show ip route, show ip route summary, show ip route database

R1

```
    #sh ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
    area
           * - candidate default

    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.10.0/24 is directly connected, eth1
    S       10.10.12.0/24 [1/0] via 10.10.10.2, eth1
    C       10.12.4.0/24 is directly connected, eth0
    C       127.0.0.0/8 is directly connected, lo
    C       192.168.0.1/32 is directly connected, lo
    S       192.168.0.2/32 [1/0] via 10.10.10.2, eth1
    S       192.168.0.3/32 [1/0] via 10.10.10.2, eth1

    #show ip route summary
    IP routing table name is Default-IP-Routing-Table(0)
```

```
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 8
Total number of IPv4 paths       : 8
Route Source    Networks
kernel          1
connected       4
static          3
Total           8
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0

---------------------------------

#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
S    *> 10.10.12.0/24 [1/0] via 10.10.10.2, eth1
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
C    *> 192.168.0.1/32 is directly connected, lo
S    *> 192.168.0.2/32 [1/0] via 10.10.10.2, eth1
S    *> 192.168.0.3/32 [1/0] via 10.10.10.2, eth1

Gateway of last resort is not set
```

R2

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
S       192.168.0.1/32 [1/0] via 10.10.10.1, eth1
```

```
C       192.168.0.2/32 is directly connected, lo
S       192.168.0.3/32 [1/0] via 10.10.12.3, eth2

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 9
Total number of IPv4 paths       : 9
Route Source    Networks
kernel          1
connected       5
static          3
Total           9
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0

---------------------------------

#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
C    *> 10.10.12.0/24 is directly connected, eth2
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
S    *> 192.168.0.1/32 [1/0] via 10.10.10.1, eth1
C    *> 192.168.0.2/32 is directly connected, lo
S    *> 192.168.0.3/32 [1/0] via 10.10.12.3, eth2

Gateway of last resort is not set
```

R3

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
```

```
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.3/32 is directly connected, lo

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 6
Total number of IPv4 paths       : 6
Route Source    Networks
kernel          2
connected       4
Total           6
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0
---------------------------------


#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
S       0.0.0.0/0 [1/0] via 10.10.12.2 inactive
C    *> 10.10.12.0/24 is directly connected, eth2
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
C    *> 192.168.0.3/32 is directly connected, lo

Gateway of last resort is not set
```

IPv6 Static Routing

This example shows complete configuration to enable IPv6 static routing in a simple network topology.

Note: IPv6 static route with interface alone as gateway (without gateway IPv6 address) is not supported.

Topology

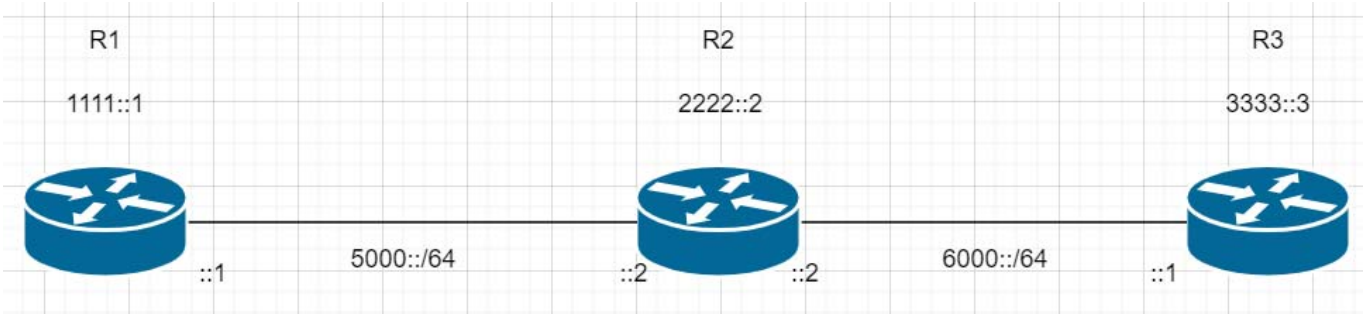


Figure 13-60: IPv6 static routing

Configuration

R1

`R1#conf t`	Enter Configure mode.
`R1(config)#interface lo`	Enter interface mode.
`R1(config-if)#ipv6 address 1111::1/128`	Configure IPv6 address
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#ipv6 route 6000::/64 5000::2`	Configure IPv6 Static route to reach remote network with R2 as nexthop
`R1(config)#ipv6 route 2222::2/128 5000::2`	Configure IPv6 static route to reach R2 lo with R2 as nexthop
`R1(config)#ipv6 route 3333::3/128 5000::2`	Configure IPv6 static route to reach R3 lo with R2 as nexthop

R2

`R2#conf t`	Enter Configure mode.
`R2(config)#int lo`	Enter interface mode.
`R2(config-if)#ipv6 address 2222::2/128`	Configure IPv6 address
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#ipv6 route 1111::1/128 5000::1`	Configure IPv6 static route to reach R1 lo with R1 as nexthop
`R2(config)#ipv6 route 3333::3/128 6000::1`	Configure IPv6 static route to reach R3 lo with R3 as nexthop

R3

`R3#conf t`	Enter Configure mode.
`R3(config)#int lo`	Enter interface mode.
`R3(config-if)#ipv6 add 3333::3/128`	Configure IPv6 address
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#ipv6 route ::/0 6000::2`	Configure Default IPv6 Static route with R2 as nexthop

Validation

show ipv6 route, show ipv6 route summary, show ipv6 route database

R1

```
R1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 20:51:02
C      1111::1/128 via ::, lo, 00:01:13
S      2222::2/128 [1/0] via 5000::2, xe3, 00:00:32
S      3333::3/128 [1/0] via 5000::2, xe3, 00:00:13
C      5000::/64 via ::, xe3, 00:01:42
S      6000::/64 [1/0] via 5000::2, xe3, 00:00:54
C      fe80::/64 via ::, ce45, 01:45:19
R1#show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths : 8
Total number of IPv6 routes      : 7
Total number of IPv6 paths       : 7
Pending routes (due to route max reached): 0
Route Source    Networks
connected       4
static          3
Total           7
FIB             7

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv6 ECMP routes   : 0
 Total number of IPv6 ECMP paths    : 0
R1#
R1#show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
       > - selected route, * - FIB route,p - stale info
Timers: Uptime

IP Route Table for VRF "default"
```

```
C   *> ::1/128 via ::, lo, 20:51:19
C   *> 1111::1/128 via ::, lo, 00:01:30
S   *> 2222::2/128 [1/0] via 5000::2, xe3, 00:00:49
S   *> 3333::3/128 [1/0] via 5000::2, xe3, 00:00:30
C   *> 5000::/64 via ::, xe3, 00:01:59
S   *> 6000::/64 [1/0] via 5000::2, xe3, 00:01:11
C   *> fe80::/64 via ::, ce45, 01:45:36
C      fe80::/64 via ::, ce44, 01:45:36
C      fe80::/64 via ::, xe39, 01:45:36
C      fe80::/64 via ::, xe32, 01:45:36
C      fe80::/64 via ::, xe29, 01:45:36
C      fe80::/64 via ::, xe13, 01:45:36
C      fe80::/64 via ::, ce46, 03:56:36
C      fe80::/64 via ::, ce43, 03:56:36
C      fe80::/64 via ::, xe25, 03:56:36
C      fe80::/64 via ::, xe23, 03:56:36
C      fe80::/64 via ::, xe3, 03:56:36
C      fe80::/64 via ::, xe34, 20:41:33
C      fe80::/64 via ::, xe33, 20:41:33
C      fe80::/64 via ::, xe36, 20:50:48
C      fe80::/64 via ::, xe22, 20:50:48
C      fe80::/64 via ::, xe21, 20:50:48
C      fe80::/64 via ::, xe10, 20:50:48
C      fe80::/64 via ::, xe9, 20:50:48
R1#
```

R2

```
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 03:59:56
S      1111::1/128 [1/0] via 5000::1, xe3, 00:00:46
C      2222::2/128 via ::, lo, 00:01:27
S      3333::3/128 [1/0] via 6000::1, xe5, 00:00:26
C      5000::/64 via ::, xe3, 00:01:52
C      6000::/64 via ::, xe5, 00:01:10
C      fe80::/64 via ::, vlan1.2, 01:17:00
R2#
R2#show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths : 8
Total number of IPv6 routes      : 7
Total number of IPv6 paths       : 7
```

```
Pending routes (due to route max reached): 0
Route Source    Networks
connected       5
static          2
Total           7
FIB             7

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv6 ECMP routes   : 0
 Total number of IPv6 ECMP paths    : 0
R2#show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
       > - selected route, * - FIB route,p - stale info
Timers: Uptime

IP Route Table for VRF "default"
C   *> ::1/128 via ::, lo, 04:00:02
S   *> 1111::1/128 [1/0] via 5000::1, xe3, 00:00:52
C   *> 2222::2/128 via ::, lo, 00:01:33
S   *> 3333::3/128 [1/0] via 6000::1, xe5, 00:00:32
C   *> 5000::/64 via ::, xe3, 00:01:58
C   *> 6000::/64 via ::, xe5, 00:01:16
C   *> fe80::/64 via ::, vlan1.2, 01:17:06
C      fe80::/64 via ::, vlan1.1, 01:17:06
C      fe80::/64 via ::, xe29, 01:48:22
C      fe80::/64 via ::, xe27, 01:48:22
C      fe80::/64 via ::, ce47, 03:59:22
C      fe80::/64 via ::, ce46, 03:59:22
C      fe80::/64 via ::, ce45, 03:59:22
C      fe80::/64 via ::, ce43, 03:59:22
C      fe80::/64 via ::, xe42, 03:59:22
C      fe80::/64 via ::, xe41, 03:59:22
C      fe80::/64 via ::, xe34, 03:59:22
C      fe80::/64 via ::, xe33, 03:59:22
C      fe80::/64 via ::, xe32, 03:59:22
C      fe80::/64 via ::, xe31, 03:59:22
C      fe80::/64 via ::, xe25, 03:59:22
C      fe80::/64 via ::, xe23, 03:59:22
C      fe80::/64 via ::, xe5, 03:59:22
C      fe80::/64 via ::, xe3, 03:59:22
R2#
```

R3

```
R3#show ipv6 route
IPv6 Routing Table
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
S      ::/0 [1/0] via 6000::2, xe5, 00:00:07
C      ::1/128 via ::, lo, 20:46:35
C      3333::3/128 via ::, lo, 00:00:57
C      6000::/64 via ::, xe5, 00:00:46
C      fe80::/64 via ::, ce43, 01:50:07
R3#show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths : 8
Total number of IPv6 routes      : 5
Total number of IPv6 paths       : 5
Pending routes (due to route max reached): 0
Route Source    Networks
connected       4
static          1
Total           5
FIB             5

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv6 ECMP routes   : 0
 Total number of IPv6 ECMP paths    : 0
R3#
R3#show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
       > - selected route, * - FIB route,p - stale info
Timers: Uptime

IP Route Table for VRF "default"
S   *> ::/0 [1/0] via 6000::2, xe5, 00:00:18
C   *> ::1/128 via ::, lo, 20:46:46
C   *> 3333::3/128 via ::, lo, 00:01:08
C   *> 6000::/64 via ::, xe5, 00:00:57
C   *> fe80::/64 via ::, ce43, 01:50:18
C      fe80::/64 via ::, xe32, 01:50:18
C      fe80::/64 via ::, xe29, 01:50:18
C      fe80::/64 via ::, xe15, 01:50:18
C      fe80::/64 via ::, xe3, 01:50:18
C      fe80::/64 via ::, ce47, 04:01:18
C      fe80::/64 via ::, ce45, 04:01:18
```

```
C      fe80::/64 via ::, xe42, 04:01:18
C      fe80::/64 via ::, xe41, 04:01:18
C      fe80::/64 via ::, xe5, 04:01:18
C      fe80::/64 via ::, xe34, 20:46:15
C      fe80::/64 via ::, xe33, 20:46:15
C      fe80::/64 via ::, xe12, 20:46:15
C      fe80::/64 via ::, xe11, 20:46:15
```

CHAPTER 14 Static Route Discard Configuration

This chapter show how to configure the static route discard feature.

Overview

If you identify some routers/attackers distributing invalid/bogus routes just to use the resources of the device or to make the device unstable, you can configure route-map rules, discard all routes, and black hole traffic corresponding to those routes.

To so this, you add “discard” route entries for a prefix in a route map with the “set interface null0” command. You then apply that route map to a BGP neighbor.

IPv4 Route Discard

Figure 14-61 shows the configuration required to enable static route discard for IPv4.

Topology

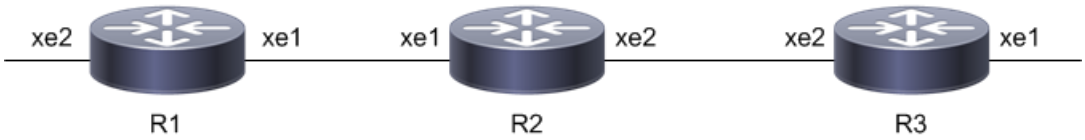


Figure 14-61: Static route discard topology

Configuration

R1

`R1#configure terminal`	Enter configure mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ip address 2.2.2.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface xe2`	Enter interface mode for xe1
`R1(config-if)#ip address 1.1.1.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#neighbor 2.2.2.3 remote-as 3`	Create static BGP neighbor 2.2.2.3 with remote autonomous system value 3
`R1(config-router)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router)#end`	Exit BGP router mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#ip prefix-list p1 permit any`	Configure IP prefix list
`R2(config)#route-map r1`	Enter route-map mode
`R2(config-route-map)#match ip address prefix-list p1`	Configure match ip prefix list p1
`R2(config-route-map)#set interface null0`	Set the interface to null0
`R2(config-route-map)#exit`	Exit route-map mode.
`R2(config)#interface xe1`	Enter interface mode for xe1
`R2(config-if)#ip address 2.2.2.3/24`	Assign an IP address to the interface
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Enter interface mode for xe2
`R2(config-if)#ip address 3.3.3.2/24`	Assign an IP address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#router bgp 3`	Enter into BGP router mode
`R2(config-router)#neighbor 2.2.2.2 remote-as 2`	Create static BGP neighbor 2.2.2.2 with remote autonomous system value 2
`R2(config-router)#neighbor 3.3.3.3 remote-as 4`	Create static BGP neighbor 3.3.3.3 with remote autonomous system value 4
`R2(config-router)#redistribute connected`	Advertise the connected network into BGP
`R2(config-router)#neighbor 2.2.2.2 route-map r1 in`	Attach the route-map with route discard configured for the neighbor 2.2.2.2 in IN direction
`R2(config-router)#end`	Exit BGP router mode

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface xe2`	Enter interface mode for xe2
`R3(config-if)#ip address 3.3.3.3/24`	Assign an IP address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#interface xe1`	Enter interface mode for xe1
`R3(config-if)#ip address 4.4.4.2/24`	Assign an IP address to the interface
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#router bgp 4`	Enter into BGP router mode
`R3(config-router)#neighbor 3.3.3.2 remote-as 3`	Create static BGP neighbor 3.3.3.2 with remote autonomous system value 3
`R3(config-router)#redistribute connected`	Advertise the connected network into BGP
`R3(config-router)#end`	Exit BGP router.

Validation

```
R2#show running-config bgp
!
```

```
router bgp 3
 redistribute connected
 neighbor 2.2.2.2 remote-as 2
 neighbor 2.2.2.2 route-map r1 in
 neighbor 3.3.3.3 remote-as 4
!

R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
       Network          Next Hop          Metric  LocPrf     Weight      Path
*>   1.1.1.0/24         2.2.2.2              0    100          0           2 ?
*>   2.2.2.0/24         0.0.0.0              0    100        32768           ?
*                       2.2.2.2              0    100          0           2 ?
*>   3.3.3.0/24         0.0.0.0              0    100        32768            ?
*                       3.3.3.3              0    100          0           4 ?
*>   4.4.4.0/24         3.3.3.3              0    100          0           4 ?
Total number of prefixes 4


R2#show running-config prefix-list
!
ip prefix-list p1 seq 5 permit any
!

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     1.1.1.0/24 [20/0] is a summary, Null, 00:00:01
C     2.2.2.0/24 is directly connected, xe1, 00:09:57
C     3.3.3.0/24 is directly connected, xe2, 00:09:50
B     4.4.4.0/24 [20/0] via 3.3.3.3, xe2, 00:00:03
C     127.0.0.0/8 is directly connected, lo, 01:18:30

Gateway of last resort is not set

R2#show hsl nh-table
IPv4 FIB 0
0.0.0.0, Null, 00:00:00:00:00:00, Valid  ,
                      1.1.1.0/24, Installed FORWARD
2.2.2.2, xe1, 00:18:23:26:16:45, Valid  , lport:0x8000026, Egress object id:1
```

```
00004, refcnt 0, rulecnt 0
3.3.3.3, xe2, 00:18:23:cb:fb:b7, Valid  , lport:0x800002a, Egress object id:1
00003, refcnt 1, rulecnt 0,
                      4.4.4.0/24, Installed FORWARD

IPv4 FIB 1 10.12.29.1, eth0, 00:00:00:00:00:00, Invalid,
                                                , Not Installed TO_CPU

IPv6 FIB 0

IPv6 FIB 1
```

IPv6 Route Discard

Figure 14-61 shows the configuration required to enable static route discard for IPv6.

Configuration

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface lo`	Enter interface mode for loopback
`R1(config-if)#ip address 1.1.1.2/24 secondary`	Assign an IPv4 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ipv6 address 2001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe2`	Enter interface mode for xe2
`R1(config-if)#ipv6 address 1001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#bgp router-id 1.1.1.1`	Specify router ID
`R1(config-router)#neighbor 2001::3 remote-as 3`	Create static BGP neighbor 2001::3 with remote autonomous system value 3
`R1(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R1(config-router-af)#neighbor 2001::3 activate`	Activate neighbor in IPv6 address family
`R1(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router)#end`	Exit BGP router mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#interface lo`	Enter interface mode for loopback
`R2(config-if)#ip address 2.2.2.2/24 secondary`	Assign an IPV4 address
`R2(config-if)#exit`	Exit interface mode
`R2(config)#ipv6 prefix-list p1 permit any`	Configure IPv6 prefix list.
`R2(config)#route-map r1`	Enter route-map mode.
`R2(config-route-map)#match ipv6 address prefix-list p1`	Configure match IPv6 prefix list p1
`R2(config-route-map)#set interface null0`	Set the interface to null0
`R2(config-route-map)#exit`	Exit route-map mode
`R2(config)#interface xe1`	Enter interface mode for xe1
`R2(config-if)#ipv6 address 2001::3/64`	Assign ipv6 address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#interface xe2`	Enter interface mode for xe2
`R2(config-if)#ipv6 address 3001::2/64`	Assign an IPv6 address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#router bgp 3`	Enter BGP router mode
`R2(config-router)#bgp router-id 2.2.2.2`	Specify router ID
`R2(config-router)#neighbor 2001::2 remote-as 2`	Create static BGP neighbor 2001::2 with remote autonomous system value 2
`R2(config-router)#neighbor 3001::3 remote-as 4`	Create static BGP neighbor 3001::3 with remote autonomous system value 4
`R2(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R2(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R2(config-router-af)#neighbor 2001::2 activate`	Activate the neighbor in IPv6 address family
`R2(config-router-af)#neighbor 3001::3 activate`	Activate the neighbor in IPv6 address family
`R2(config-router-af)#neighbor 2001::2 route-map r1 in`	Attach the route-map with route discard configured for the neighbor 2001::2 in IN direction
`R2(config-router)#end`	Exit BGP router mode

R3

`R3#configure terminal`	Enter configure mode
`R3(config)#interface lo`	Enter interface mode for loopback
`R3(config-if)#ip address 3.3.3.2/24 secondary`	Assign an IPV4 address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#interface xe1`	Enter interface mode for xe1
`R3(config-if)#ipv6 address 4001::2/64`	Assign an IPv6 address to the interface

R3(config-if)#exit	Exit interface mode
R3(config)#interface xe2	Enter interface mode for xe2
R3(config-if)#ipv6 address 3001::3/64	Assign an IPv6 address to the interface
R3(config-if)#exit	Exit interface mode
R3(config)#router bgp 4	Enter into BGP router mode
R3(config-router)#bgp router-id 3.3.3.3	Specify router ID
R3(config-router)#neighbor 3001::2 remote-as 3	Create static BGP neighbor 3001::2 with remote autonomous system value 3
R3(config-router)#address-family ipv6 unicast	Enter address family IPv6 unicast mode
R3(config-router-af)#neighbor 3001::2 activate	Activate neighbor in IPv6 address family
R3(config-router-af)#redistribute connected	Advertise the connected network into BGP
R3(config-router)#end	Exit BGP router mode.

Validation

```
R2#show running-config bgp
!
router bgp 3
 bgp router-id 2.2.2.2
 neighbor 2001::2 remote-as 2
 neighbor 3001::3 remote-as 4
 !
 address-family ipv6 unicast
 redistribute connected
 neighbor 2001::2 activate
 neighbor 2001::2 route-map r1 in
 neighbor 3001::3 activate
 exit-address-family
!
R2#show  bgp ipv6
BGP table version is 3, local router ID is 2.2.2.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network    Next Hop                            Metric  LocPrf  Weight  Path
*> 1001::/64 2001::2(fe80::218:23ff:fede:eecf)
                                                    0      100      0        2?
*> 2001::/64  ::                                    0      100    32768       ?
*            2001::2(fe80::218:23ff:fede:eecf)
                                                    0      100      0        2?
*> 3001::/64  ::                                    0      100     32768      ?
*            3001::3(fe80::eef4:bbff:fe84:781b)  0      100       0       4? *> 4001::/
64 3001::3(fe80::eef4:bbff:fe84:781b)  0      100       0       4?

Total number of prefixes 4
```

```
R2#show running-config ipv6 prefix-list
!
ipv6 prefix-list p1 seq 5 permit any
!

R2#

R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:56:44
B      1001::/64 [20/0] via ::, Null, 00:00:04
C      2001::/64 via ::, xe1, 00:13:03
C      3001::/64 via ::, xe2, 00:12:56
B      4001::/64 [20/0] via fe80::eef4:bbff:fe84:781b, xe50, 00:00:02
C      fe80::/64 via ::, xe50, 00:46:14


R2#show hsl nh-table
IPv4 FIB 0

IPv4 FIB 1
10.12.29.1, eth0, 00:00:00:00:00:00, Invalid,
                      , Not Installed TO_CPU

IPv6 FIB 0
  , Null, 00:00:00:00:00:00, Valid  ,
                      1001::/64, Installed FORWARD
2001::2, xe1, 00:18:23:de:ee:cf, Valid  , lport:0x8000034, Egress object id:100003,
refcnt 0, rulecnt 0
3001::3, xe2, ec:f4:bb:84:78:1b, Valid  , lport:0x8000032, Egress object id:100004,
refcnt 0, rulecnt 0
fe80::218:23ff:fede:eecf, xe52, 00:18:23:de:ee:cf, Valid  , lport:0x8000034, Egress
object id:100003, refcn
t 0, rulecnt 0
fe80::eef4:bbff:fe84:781b, xe50, ec:f4:bb:84:78:1b, Valid  , lport:0x8000032, Egress
object id:100004, refc
nt 1, rulecnt 0,
                      4001::/64, Installed FORWARD

IPv6 FIB 1
```

CHAPTER 15 Layer 3 Subinterface Configuration

This chapter contains examples of configuring subinterfaces.

A subinterface is a virtual interface created by dividing one physical interface into multiple logical interfaces. A subinterface in a router uses the parent physical interface for sending and receiving data.

Subinterfaces are used for a variety of purposes. If you have one router with one physical interface, but need to connect the router to two IP networks to route traffic between two routers, you can create two subinterfaces within the physical interface, assign each subinterface an IP address within each subnet, and then route the data between two subnets.

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN identifiers. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances.

Note: Refer to the release note for features supported by L3 Sub-interface.

Topology

Figure 15-62 shows and example of subinterface configuration. In this example, there are two routers, R1 and R2, and the eth1 interface of R1 is connected directly to eth2 of R2 using an Ethernet cable.

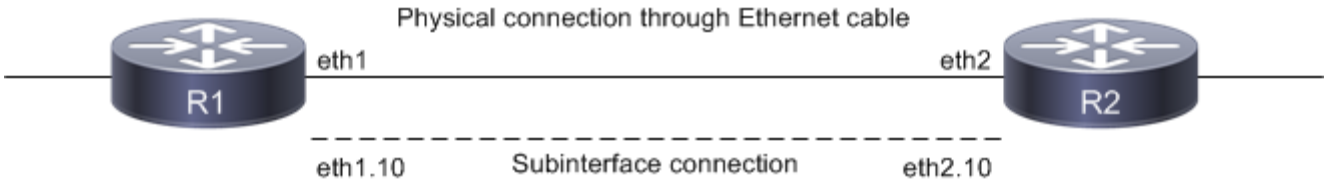


Figure 15-62: Subinterface connections

The eth1.10 subinterface is created on R1, and eth2.10 is created on R2.

Note: Subinterfaces can be created on physical and LAG interfaces in Layer 3 mode (`no switchport`).

Creating a Subinterface

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#interface eth1.10`	Creates a sub-interface as eth1.10
`(config-if)#encapsulation dot1q 10`	Configure the encapsulation as dot1q matching vlan 10
`(config-if)#ip address 10.10.10.1/24`	Assigning IP address to sub-interface
`(config-if)#exit`	Exit interface mode

Creating a Subinterface with Encapsulation

Double encapsulation as dot1q

```
#configure terminal (config)#interface eth1.1010
(config-if)# encapsulation dot1q 10 inner-dot1q 10
(config-if)#ip address 192.168.1.50/24
```

Double encapsulation as dot1ad

```
#configure terminal (config)#interface eth1.20
(config-if)# encapsulation dot1ad 20 inner-dot1q 20
(config-if)#ip address 192.168.2.50/24
```

Note: Use `switchport dot1q ethertype (8100 | 88a8 | 9100 | 9200)`command to configure the service-tpid value on parent port of a subinterface. By this the tpid used for service tag for a subinterface may be inherited from the one applied to parent interface.

Note: For any dot1ad subinterface to be functional, switchport dot1q ethertype should be set to desired value as 88a8/9100/9200. Default value is 8100. To verify the ethertype value for the interface use `show interface <subinterface>` command.

Displaying Subinterfaces

In OcNOS, subinterfaces appear as any physical interface in the `show running-coccnfig` or the show ip interface brief output and can be configured as any other interface.

The following examples display subinterface information from various `show` commands.

Note: The below command output is just for reference and is not directly related to the configuration provided above

show interface brief

```
RTR1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,       PD(Min-links) -
Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type  PVID  Mode             Status  Reason  Speed Port
Interface                                                   Ch #
--------------------------------------------------------------------------------
ce49       ETH   --    routed           up      none    100g  --


--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
```

```
--------------------------------------------------------------------------------
ce49.2        SUBINTERFACE     up      --     0
ce49.3        SUBINTERFACE     up      --     0
ce49.4        SUBINTERFACE     up      --     0
ce49.5        SUBINTERFACE     up      --     0
ce49.6        SUBINTERFACE     up      --     0
```

show ip interface brief

```
RTR1#show ip interface brief

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
ce49                 unassigned      up                    up
ce49.2               49.49.2.1       up                    up
ce49.3               49.49.3.1       up                    up
ce49.4               49.49.4.1       up                    up
ce49.5               49.49.5.1       up                    up
ce49.6               49.49.6.1       up                    up
```

show ip ospf neighbor with VRF enabled

```
RTR1#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
4.4.4.4           1   Full/DR         00:00:32    48.48.2.2       vlan1.2               0
4.4.4.4           1   Full/DR         00:00:38    48.48.3.2       vlan1.3               0

Total number of full neighbors: 1
OSPF process 2 VRF(CUST-2):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
11.11.2.1         1   Full/DR         00:00:39    49.49.2.2       ce49.2                0

Total number of full neighbors: 1
OSPF process 3 VRF(CUST-3):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
11.11.3.1         1   Full/Backup     00:00:33    49.49.3.2       ce49.3
0

Total number of full neighbors: 1
OSPF process 4 VRF(CUST-4):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
11.11.4.1         1   Full/Backup     00:00:31    49.49.4.2       ce49.4
0

Total number of full neighbors: 1
OSPF process 5 VRF(CUST-5):
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
11.11.5.1         1   Full/Backup     00:00:39    49.49.5.2       ce49.5
0
```

show ip route with VRF enabled

```
RTR1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.2.200.0/24 is directly connected, xe1.200, 01:29:19
O            4.4.4.4/32 [110/11] via 48.48.3.2, vlan1.3, 00:37:17
                        [110/11] via 48.48.2.2, vlan1.2
O            44.44.44.0/24 [110/2] via 48.48.3.2, vlan1.3, 00:37:17
                           [110/2] via 48.48.2.2, vlan1.2
C            47.47.2.0/24 is directly connected, xe47.2, 00:34:42
C            48.48.2.0/24 is directly connected, vlan1.2, 00:41:19
C            48.48.3.0/24 is directly connected, vlan1.3, 00:41:19
C            127.0.0.0/8 is directly connected, lo, 01:30:09

Gateway of last resort is not set

RTR1#show ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.2.200.0/24 is directly connected, xe1.200, 01:29:32
O            4.4.4.4/32 [110/11] via 48.48.3.2, vlan1.3, 00:37:30
                        [110/11] via 48.48.2.2, vlan1.2
O            44.44.44.0/24 [110/2] via 48.48.3.2, vlan1.3, 00:37:30
                           [110/2] via 48.48.2.2, vlan1.2
C            47.47.2.0/24 is directly connected, xe47.2, 00:34:55
C            48.48.2.0/24 is directly connected, vlan1.2, 00:41:32
C            48.48.3.0/24 is directly connected, vlan1.3, 00:41:32
C            127.0.0.0/8 is directly connected, lo, 01:30:22
IP Route Table for VRF "management"
C            127.0.0.0/8 is directly connected, lo.management, 01:30:22
C            192.168.10.0/24 is directly connected, eth0, 01:30:22
IP Route Table for VRF "CUST-1"
C            127.0.0.0/8 is directly connected, lo.CUST-1, 01:30:22
IP Route Table for VRF "CUST-2"
```

```
C            1.1.2.0/24 is directly connected, xe1.2, 01:29:35
C            1.2.101.0/24 is directly connected, xe1.101, 01:29:34
C            1.3.201.0/24 is directly connected, xe1.201, 01:29:32
O            11.11.2.0/24 [110/20] via 49.49.2.2, ce49.2, 00:51:06
O            11.12.101.0/24 [110/20] via 49.49.2.2, ce49.2, 00:51:06
O            11.13.201.0/24 [110/20] via 49.49.2.2, ce49.2, 00:51:06
C            49.49.2.0/24 is directly connected, ce49.2, 01:29:31
C            127.0.0.0/8 is directly connected, lo.CUST-2, 01:30:22
IP Route Table for VRF "CUST-3"
C            1.1.3.0/24 is directly connected, xe1.3, 01:29:35
C            1.2.102.0/24 is directly connected, xe1.102, 01:29:34
C            1.3.202.0/24 is directly connected, xe1.202, 01:29:32
O            11.11.3.0/24 [110/20] via 49.49.3.2, ce49.3, 01:12:44
O            11.12.102.0/24 [110/20] via 49.49.3.2, ce49.3, 01:12:44
O            11.13.202.0/24 [110/20] via 49.49.3.2, ce49.3, 01:12:44
C            49.49.3.0/24 is directly connected, ce49.3, 01:29:31
```

CHAPTER 16 Two-way Active Measurement Protocol

Two-way Active Measurement Protocol (TWAMP) is an open protocol for measuring network performance between any two devices:

- The TWAMP control protocol sets up performance measurement sessions.
- The TWAMP test protocol sends and receives performance measurement probes.

The control client initiates all requested test sessions with a start session message, and the server acknowledges. When necessary, the control client sends a message to stop all test sessions.

The session sender and the session reflector exchange test packets according to the TWAMP test protocol for each active session. On receiving a TWAMP test packet, the session reflector only reflects a measurement packet and does not collect packet statistics in TWAMP.

TWAMP control can have eight TWAMP sessions on the device and reflector can serve up to eight TWAMP sessions on the reflector device.

This chapter shows a configuration using TWAMP “light” mode.

Topology

Figure 16-63: TWAMP topology

Configuring L3 Reachability between Router1 and Router3

Router 1

`ROUTER1#conf terminal`	Enter to Config mode
`ROUTER1(config)#hostname ROUTER1`	Entering the device name
`ROUTER1(config)#in xe1`	Entering into interface xe1
`ROUTER1(config-if)#ip address 10.10.10.1/24`	Configuring ip address
`ROUTER1(config-if)#ex`	Exit from interface mode
`ROUTER1(config)#in lo`	Entering into interface lo
`ROUTER1(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address to lo interface
`ROUTER1(config-if)#exit`	Exit from lo interface
`ROUTER1(config)#router ospf 1`	Configure ospf process id

`ROUTER1(config-router)#router-id 1.1.1.1`	Configure router id
`ROUTER1(config-router)#network 10.10.10.0 0.0.0.255 area 0`	Configure the network's in ospf
`ROUTER1(config-router)#network 1.1.1.0 0.0.0.255 area 0`	Configure the network's in ospf

Router 2

`ROUTER2#conf terminal`	Enter to Configure mode
`ROUTER2(config)#hostname ROUTER2`	Entering the device name
`ROUTER2(config)#in xe1`	Entering into interface xe1
`ROUTER2(config-if)#ip address 10.10.10.2/24`	Configuring ip address
`ROUTER2(config-if)#ex`	Exit from interface mode
`ROUTER2(config)#in xe2`	Entering into interface xe2
`ROUTER2(config-if)#ip address 20.20.20.1/24`	Configuring ip address
`ROUTER2(config-if)#ex`	Exit from interface mode
`ROUTER2(config)#in lo`	Entering into interface lo
`ROUTER2(config-if)#ip address 2.2.2.2/32 secondary`	Configure ip address to lo interface
`ROUTER2(config-if)#exit`	Exit from lo interface
`ROUTER2(config)#router ospf 2` `ROUTER2(config)#router-id 2.2.2.2`	Configure ospf process id and router-id
`ROUTER2(config-router)#network 10.10.10.0 0.0.0.255 area 0`	Configure the network's in ospf
`ROUTER2(config-router)#network 20.20.20.0 0.0.0.255 area 0`	Configure the network's in ospf
`ROUTER2(config-router)#network 2.2.2.0 0.0.0.255 area 0`	Configure the network's in ospf

Router 3

`ROUTER3#conf terminal`	Enter to Config mode
`ROUTER3(config)#hostname ROUTER3`	Entering the device name
`ROUTER3(config)#in xe2`	Entering into interface xe2
`ROUTER3(config-if)#ip address 20.20.20.2/24`	Configuring ip address
`ROUTER3(config-if)#ex`	Exit from interface mode
`ROUTER3(config)#in lo`	Entering into interface lo
`ROUTER3(config-if)#ip address 3.3.3.3/32 secondary`	Configure ip address to lo interface

ROUTER3(config-if)#exit	Exit from lo interface
ROUTER3(config)#router ospf 3	Configure ospf process id
ROUTER3(config-router)#router-id 3.3.3.3	Configure router id
ROUTER3(config-router)#network 20.20.20.0 0.0.0.255 area 0	Configure the network's in ospf
ROUTER3(config-router)#network 3.3.3.0 0.0.0.255 area 0	Configure the network's in ospf

Configuring TWAMP on the Router

Router 1

ROUTER1#configure terminal	Enter Configure mode
ROUTER1(config)#twamp-light control	Enter to Twamp-Light control mode
ROUTER1(config-twamp-light-ctrl)#control-admin-state enable	Enabling the Twamp-light Control
ROUTER1(config-twamp-light-ctrl)#test-session-name s1 sender-ip 1.1.1.1 sender-port 1300 reflector-ip 3.3.3.3 reflector-port 1301	Configuring the Twamp Test-Session

Router 3

ROUTER3#configure terminal	Enter Configure mode
ROUTER3(config)#twamp-light reflector	Enter to Twamp-Light reflector mode
ROUTER3(config-twamp-light-ref)#reflector-admin-state enable	Enabling Twamp-light reflector
ROUTER3(config-twamp-light-ref)#reflector-ip 3.3.3.3 reflector-port 1301	Configuring the reflector ip and port number

Start the Twamp-session on ROUTER1:

`ROUTER1#twamp start test-session s1 packet-count 50 interval 500`	Starting the Twamp Test-session on Twamp-Control device

Stop the Twamp-session on ROUTER1

`ROUTER1#twamp stop test-session s1`	Stop the Twamp Test-session on Twamp-Control device

Disabling the TWAMP-Control on ROUTER1

`ROUTER1#configure terminal`	Enter Configure mode
`ROUTER1(config)#twamp-light control`	Enter to Twamp-Light control mode
`ROUTER1(config-twamp-light-ctrl)#control-admin-state disable`	Disable the Twamp-light Control

Disabling the TWAMP-Reflector on ROUTER3

Remove/Un-config of Test Session

`ROUTER3#configure  terminal`	Enter Configure mode
`ROUTER3(config)#twamp-light reflector`	Enter to Twamp-Light reflector mode
`ROUTER3(config-twamp-light-ref)#reflector-admin-state disable`	Disable the Twamp-light reflector

`ROUTER1#configure terminal`	Enter Configure mode
`ROUTER1(config)#twamp-light control`	Enter to Twamp-Light control mode
`ROUTER1(config-twamp-light-ctrl)#no test-session name s1`	Removing/un-configuring of Twamp Test Session

Remove/Un-config of TWAMP-Control

ROUTER1#configure terminal	Enter Configure mode
ROUTER1(config)#no twamp-light control	Removing/un-configuring of Twamp control

Remove/Un-Config of TWAMP-Reflector

ROUTER3#configure terminal	Enter Configure mode
ROUTER3(config)#no twamp-light reflector	Removing/un-configuring of Twamp reflector

Validation

```
ROUTER1#show running-config twamp
ROUTER1#show twamp-statistics
```

Validation of configuration on Twamp-Reflector

```
ROUTER1#sh running-config twamp
twamp-light reflector
 reflector-admin-state enable
 reflector-ip 3.3.3.3 reflector-port 1301
```

Validation of configuration on Twamp-Control

```
ROUTER1#sh running-config twamp
twamp-light control
 control-admin-state enable
 test-session-name s1 sender-ip 1.1.1.1 sender-port 1300 reflector-ip 3.3.3.3
reflector-port 1301
```

Validation of Twamp-session packets on Twamp-Control

```
R1#show twamp-statistics s1
========================================
TWAMP Test-Session Statistics
========================================
Test-Session Name : s1
Start Time : 2019 Aug 06 08:57:05
Elapsed time(milli sec) : 25040
Packets Sent : 50
Packets Received : 50
Packet Loss(%) : 0.0000
Round Trip Delay(usec)
Minimum : 225
Maximum : 13462
Average : 558
Forward Delay(usec)
Minimum : 155
Maximum : 1372
Average : 211
Reverse Delay(usec)
Minimum : 38
Maximum : 13291
Average : 346
Round Trip Delay Variation(usec)
Minimum : 326
```

```
    Maximum : 13655
    Average : 4200
    Forward Delay Variation(usec)
    Minimum : 185
    Maximum : 2925
    Average : 986
    Reverse Delay Variation(usec)
    Minimum : 141
    Maximum : 11551
    Average : 3441
```

Border Gateway Protocol Command Reference

Contents

This document contains these chapters and appendices:

CHAPTER 1 BGP Commands

This chapter describes the BGP configuration commands.

- bgp table-map
- clear bgp (A.B.C.D|X:X::X:X)
- clear bgp *
- clear bgp <1-4294967295>
- clear bgp dampening
- clear bgp external
- clear bgp flap-statistics
- clear bgp peer-group
- clear bgp statistics
- clear bgp view
- clear ip bgp A.B.C.D
- clear ip bgp A.B.C.D vrf
- clear ip bgp A.B.C.D ipv4 labeled-unicast
- clear ip bgp peer-group WORD ipv4 labeled-unicast
- clear ip bgp * ipv4 labeled-unicast
- clear ip bgp table-map
- debug bgp
- distance bgp
- exit-address-family
- ip as-path access-list
- ip community-list <1-99>
- ip community-list <100-500>
- ip community-list expanded
- ip community-list standard
- ip community-list WORD
- ip extcommunity-list <1-99>
- ip extcommunity-list <100-500>
- ip extcommunity-list expanded
- ip extcommunity-list standard
- match ip peer
- max-paths
- neighbor activate
- neighbor additional-paths
- neighbor advertise additional-paths
- neighbor advertisement-interval
- neighbor allowas-in
- neighbor as-origination-interval
- neighbor attribute-unchanged
- neighbor capability dynamic

- neighbor capability orf prefix-list
- neighbor capability route-refresh
- neighbor collide-established
- neighbor connection-retry-time
- neighbor default-originate
- neighbor description
- neighbor disallow-infinite-holdtime
- neighbor distribute-list
- neighbor dont-capability-negotiate
- neighbor ebgp-multihop
- neighbor enforce-multihop
- neighbor fall-over bfd
- neighbor filter-list
- neighbor limit
- neighbor local-as
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor optional-as
- neighbor override-capability
- neighbor passive
- neighbor authentication-key
- neighbor peer-group
- neighbor port
- neighbor prefix-list
- neighbor remote-as
- neighbor remove-private-AS
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-server-client
- neighbor send-community
- neighbor send-label explicit-null
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor strict-capability-match
- neighbor timers
- neighbor transparent-as
- neighbor transparent-nexthop
- neighbor unsuppress-map
- neighbor update-source

- neighbor version
- neighbor weight
- neighbor WORD peer-group
- network
- network synchronization
- redistribute
- router bgp
- snmp restart bgp
- synchronization
- timers bgp

address-family

Use the address family command to enter the IPv4 or VPNv4 address family mode allowing configuration of address-family specific parameters. To leave address family mode and return to configure mode, give the exit-address-family command.

This command configures the routing exchange between Provider Edge (PE) and Customer Edge (CE) devices. The BGP sessions between PE routers can carry different types of routes (VPN-IPv4 and IPv4 routes). Address families are used to control the type of BGP session. Configure a BGP address family for each VRF configured on the PE router and a separate address family to carry VPN-IPv4 routes between PE routers. All non VPN BGP neighbors are defined using router mode. All VPN BGP neighbors are defined under its associated address family mode. The BGP process with no address-family specified is the default address-family, where any sessions are configured that either are not associated with a VRF or are used to carry IPv4 routes.

Use the no parameter with this command to disable the address-family configurations.

Command Syntax

```
address-family ipv4
address-family ipv4 (unicast|multicast)
address-family ipv4 vrf NAME
address-family ipv4 labeled-unicast
address-family ipv6 labeled-unicast
address-family l2vpn evpn
address-family rtfilter unicast
address-family vpn4
address-family vpn4 unicast
address-family vpnv6
address-family vpnv6 unicast
no address-family ipv4 vrf NAME
no address-family ipv4 multicast
no address-family l2vpn evpn
no address-family rtfilter unicast
no address-family vpnv4
no address-family vpnv4 unicast
no address-family vpnv6
no address-family vpnv6 unicast
```

Parameters

ipv4	IPv4 address family
unicast	Unicast address prefixes
multicast	Multicast address prefixes
vrf	Virtual Private Network (VPN) routing/forwarding instance
NAME	VPN routing/forwarding instance name

`unicast`	Unicast address prefixes
`labeled-unicast`	Enter IPv4 labeled-unicast address-family mode to advertise labeled unicast routes. When a neighbor activate command is given in this mode, the BGP speaker advertises the BGP-LU capability.
`ipv6`	IPv6 address family
`labeled-unicast`	Enter IPv6 labeled-unicast address-family mode to: Activate an IPv4 neighbor to exchange labeled routes data among ISP PE devices. When a IPv4 neighbor activate command is given in this mode, the device becomes 6PE capable. OR: Activate an IPv6 neighbor to advertise labeled unicast routes. When a IPv6 neighbor activate command is given in this mode, the BGP speaker advertises the BGP-LU capability.
`l2vpn evpn`	Layer 2 VPN routing sessions with EVPN endpoint information distributed to BGP peers
`rtfilter`	Route target filter: on an iBGP peer or Route Reflector (RR), only send IPv4 and IPv6 prefixes to PE routers when a PE has a VRF that imports those specific prefixes.
`unicast`	Unicast address prefixes
`vpnv4`	VPN version 4 address family
`unicast`	Unicast address prefixes
`vpnv6`	VPN version 6 address family
`unicast`	Unicast address prefixes

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#neighbor 3ffe:506::1 remote-as 7657
(config-router)#neighbor 3ffe:506::1 interface eth1

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4
(config-router-af)#neighbor 3ffe:506::1 activate
(config-router-af)#exit-address-family
```

Note:

For 6PE address family, the following commands are not supported.

- table-map filter

In addition, the following neighbor command options are also not supported for 6PE:

- Allow-as in
- attribute-unchanged
- distribute-list
- filter-list
- maximum-prefix
- default-originate

aggregate-address

Use this command to configure BGP aggregate entries.

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route.The `aggregate-address` command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the `summary-only` parameter advertises the prefix only, suppressing the more-specific routes to all neighbors. In the following example Router1 will propagate network 172.0.0.0 and suppresses the more specific route 172.10.0.0.

The `as-set` parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use this parameter to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. The `as-set` parameter is useful when aggregation of information results in an incomplete path information.

Use the no parameter with this command to disable this function.

Command Syntax

```
aggregate-address A.B.C.D/M
aggregate-address A.B.C.D/M as-set
aggregate-address A.B.C.D/M as-set summary-only
aggregate-address A.B.C.D/M summary only
aggregate-address A.B.C.D/M summary-only as-set
no aggregate-address A.B.C.D/M
no aggregate-address A.B.C.D/M as-set
no aggregate-address A.B.C.D/M as-set summary-only
no aggregate-address A.B.C.D/M summary only
no aggregate-address A.B.C.D/M summary-only as-set
```

Parameters

`A.B.C.D/M`	Aggregate prefix
`as-set`	Generate AS set path information
`summary-only`	Filter more specific routes from updates

Default

By default, aggregate address A.B.C.D/M is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#aggregate-address 10.0.0.0/8 as-set summary-only
```

```
(config)#router bgp 100
(config-router)#no aggregate-address 10.0.0.0/8 as-set summary-only
```

auto-summary

Use this command to enable sending summarized routes by a BGP speaker to its peers in the router configuration mode or in the address-family configuration mode. Auto-summary is used by a BGP router to advertise summarized routes to its peers. Auto-summary can be enabled if certain routes have already been advertised: in this case, configuring auto-summary advertises the summarized routes first, then corresponding non-summarized routes are withdrawn. If certain routes have already been advertised, and auto-summary is disabled, non-summarized routes are first advertised, then the corresponding summarized routes are withdrawn from all the connected peers.

Use the no parameter with this command to disable this function.

Command Syntax

```
auto-summary
no auto-summary
```

Parameters

None

Default

By default, auto-summary is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables auto-summary in Router mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#auto-summary
```

The following example enables auto-summary using the IPv4 address family.

```
#configure terminal
(config)#router bgp 1
(config)#address-family ipv4
(config-af)#auto-summary
```

bgp additional-paths

Use this command to enable BGP add-path.

Use the no parameter with this command to disable BGP add-path.

Command Syntax

```
bgp additional-paths (send|receive|send-receive)
no bgp additional-paths (send|receive|send-receive)
```

Parameters

`send`	Send additional paths to neighbors
`receive`	Receive additional paths from neighbors
`send-receive`	Send and Receive additional paths from neighbors

Default

By default, bgp additional-paths is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#bgp additional-paths send

(config-router)#no bgp additional-paths send
```

bgp additional-paths select

Use this command to enable BGP add-path advertisement.

Use the no parameter with this command to disable BGP add-path advertisement.

Command Syntax

```
bgp additional-paths select (all|best <2-3>)
no bgp additional-paths select (all|best <2-3>)
```

Parameters

`all`	Select all available paths
`best`	Select best N paths
`<2-3>`	Number of best paths in additional paths to be selected

Default

By default, bgp additional-paths select is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#bgp additional-paths select all

(config-router)#no bgp additional-paths select all
```

bgp aggregate-nexthop-check

Use this command to set the BGP option to perform aggregation only when next-hop matches the specified IP address.

Use the no parameter with this command to disable this functionality.

Command Syntax

```
bgp aggregate-nexthop-check
no bgp aggregate-nexthop-check
```

Parameters

None

Default

By default, bgp aggregate nexthop check is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp aggregate-nexthop-check
```

bgp always-compare-med

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. MED comparison is done only among paths from the same autonomous system (AS). Use `bgp always-compare-med` command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred. If the bgp table shows the following and the always-compare-med is enabled:

```
Route1: as-path 400, med 300
Route2: as-path 200, med 200
Route3: as-path 400, med 250
```

Route1 is compared to Route2. Route2 is best of the two (lower MED). Next, Route2 is compared to Route3 and Route2 is chosen best path again (lower MED). If always-compare-med was disabled, MED is not taken into account when Route1 and Route2 are compared, because of different ASs and MED is compared for only Route1 and Route3. In this case, Route3 would be the best path. The selected route is also affected by the `bgp deterministic-med` command. Please see `bgp deterministic-med` command for details. If this command is used to compare MEDs for all paths, it should be configured on every BGP router in the AS.

Use the `no` parameter with this command to disallow the comparison.

Command Syntax

```
bgp always-compare-med
```

```
no bgp always-compare-med
```

Parameters

None

Default

By default, bgp always compare med is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp always-compare-med
```

bgp as-local-count

Use this command to set the number of times the local-AS (Autonomous System) is to be prepended.

Use the no parameter with this command to stop prepending the local AS count.

Command Syntax

```
bgp as-local-count <2-64>
no bgp as-local-count <2-64>
```

Parameter

<2-64>	The number of times the local-AS is to be prepended

Default

By default, bgp as local count is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp as-local-count 55

(config)#router bgp 100
(config-router)#no bgp as-local-count 55
```

bgp bestpath as-path ignore

Use this command to prevent the router from considering the autonomous system (AS) path length as a factor in the algorithm for choosing a best path route.

Use the no parameter with this command to allow the router to consider the AS path length in choosing a best path route.

Command Syntax

```
bgp bestpath as-path ignore
no bgp bestpath as-path ignore
```

Parameters

None

Default

By default, bgp bestpath as-path ignore is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path ignore

(config)#router bgp 100
(config-router)#no bgp bestpath as-path ignore
```

bgp bestpath as-path multipath-relax

Use this command to relax the “same AS-Path” requirement so any candidate eBGP AS-Path with the same AS-path length might be used for eBGP load-balancing.

Note: This feature does not load-balance between eBGP and iBGP paths.

Normally eBGP load-balancing requires the candidate routes to be equal-cost paths with identical BGP attributes having the same weight, Local-Pref, AS-Path (both the AS numbers and the AS path length), origin, MED, and different next-hop.

Use the no parameter with this command to return to normal operation.

Command Syntax

```
bgp bestpath as-path multipath-relax
no bgp bestpath as-path multipath-relax
```

Parameters

None

Default

By default, as-path multipath-relax is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path multipath-relax

(config)#router bgp 100
(config-router)#no bgp bestpath as-path multipath-relax
```

bgp bestpath compare-confed-aspath

Use this command to allow comparing of the confederation AS path length. This command specifies that the AS confederation path length must be used when available in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been used.

Use the no parameter with this command to ignore consideration of AS confederation path length in BGP best path selection.

Command Syntax

```
bgp bestpath compare-confed-aspath
no bgp bestpath compare-confed-aspath
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-confed-aspath

(config)#router bgp 100
(config-router)#no bgp bestpath compare-confed-aspath
```

bgp bestpath compare-routerid

Use this command to compare router IDs for identical eBGP paths. When comparing similar routes from peers, the BGP router does not consider the router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with the lowest router ID is selected. The router IS is the highest IP address on the router, with preference given to loopback addresses. Router ID can be manually set by using the bgp router-id command.

Use the no parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath compare-routerid
```

```
no bgp bestpath compare-routerid
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-routerid

(config)#router bgp 100
(config-router)#no bgp bestpath compare-routerid
```

bgp bestpath dont-compare-originator-id

Use this command to change the default bestpath selection by not comparing an originator-ID for an identical EBGP path.

Use the no parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath dont-compare-originator-id
```

```
no bgp bestpath dont-compare-originator-id
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath dont-compare-originator-id

(config)#router bgp 100
(config-router)#no bgp bestpath dont-compare-originator-id
```

bgp bestpath med

Use this command to specify two MED (Multi Exit Discriminator) attributes, `confed` and `missing-as-worst`.

The `confed` attribute enables MED comparison along paths learned from confederation peers. The MEDs are compared only if there is no external Autonomous System (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made. For example in the following paths, the MED is not compared with Route3 as it is not in the confederation. MED is compared for Route1 and Route2 only.

```
Path1 = 32000 32004, med=4
Path2 = 32001 32004, med=2
Path3 = 32003 1, med=1
```

The `missing-as-worst` attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If `missing-as-worst` is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Use the `no` parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax

```
bgp bestpath med confed missing-as-worst
bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med)
bgp bestpath med missing-as-worst confed
no bgp bestpath med confed missing-as-worst
no bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med)
no bgp bestpath med missing-as-worst confed
```

Parameters

`confed`	Compare MED along confederation paths
`missing-as-worst`	Treat missing MED as the least preferred one
`remove-recv-med`	Remove received MED attribute
`remove-send-med`	Remove sent MED attribute

Command Mode

Router mode

Default

By default, MED value is zero.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```

```
(config)#router bgp 100
(config-router)#bgp bestpath med missing-as-worst

(config)#router bgp 100
(config-router)#bgp bestpath med remove-recv-med
(config-router)#no bgp bestpath med remove-recv-med

(config)#router bgp 100
(config-router)#bgp bestpath med remove-send-med
(config-router)#no bgp bestpath med remove-send-med
```

bgp bestpath tie-break-on-age

Use this command to always select a preferred older route even when the `bgp bestpath compare-routerid` command is configured.

Use the `no` parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath tie-break-on-age
```

```
no bgp bestpath tie-break-on-age
```

Parameters

None

Default

By default, tie-break-on-age is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath tie-break-on-age

(config)#router bgp 100
(config-router)#no bgp bestpath tie-break-on-age
```

bgp client-to-client reflection

Use this command to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use `no bgp client-to-client reflection` command to disable the client-to-client route reflection.

Use the no parameter with this command to turn off client-to-client reflection.

Command Syntax

```
bgp client-to-client reflection
no bgp client-to-client reflection
```

Parameters

None

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp client-to-client reflection

(config)#router bgp 100
(config-router)#no bgp client-to-client reflection
```

bgp cluster-id

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The `bgp cluster-id` command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Use the `no` parameter with this command (without any arguments) to remove a previously configured route reflector cluster ID.

Command Syntax

```
bgp cluster-id <1-4294967295>
bgp cluster-id A.B.C.D
no bgp cluster-id
```

Parameters

`<1-4294967295>`	Route reflector ID as a 32-bit quantity
`A.B.C.D`	Route reflector ID in an IPv4 address format

Default

By default, cluster id is set bgp cluster id

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following configuration creates a cluster-id 5 including two route-reflector-clients.

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 3.3.3.3 route-reflector-client
(config-router)#neighbor 5.5.5.5 remote-as 200
(config-router)#neighbor 5.5.5.5 route-reflector-client
(config-router)#neighbor 6.6.6.6 remote-as 200
(config-router)#bgp cluster-id 5
```

bgp confederation identifier

Use this command to specify a BGP confederation identifier.

Use the no parameter with this command to remove a BGP confederation identifier.

Command Syntax

```
bgp confederation identifier <1-65535>
no bgp confederation identifier
```

Parameter

<1-65535>	Routing domain confederation AS number

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 1
```

bgp confederation peers

Use this command to configure the Autonomous Systems (AS) that belong to a confederation. A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External BGP (eBGP) routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation.

Use the no parameter with this command to remove an autonomous system from the confederation.

Command Syntax

```
bgp confederation peers <1-65535>
no bgp confederation peers <1-65535>
```

Parameter

<1-65535>	AS numbers of eBGP peers that are in the same confederation

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration example, the neighbor 172.210.30.2 and 172.210.20.1 have iBGP connection within AS 100, neighbor 173.213.30.1 is a BGP connection with a confederation peer 200 and neighbor 6.6.6.6 has an eBGP connection to external AS 300.

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 300
(config-router)#bgp confederation peers 200
(config-router)#neighbor 172.210.30.2 remote-as 100
(config-router)#neighbor 172.210.20.1 remote-as 100
(config-router)#neighbor 173.213.30.1 remote-as 200
(config-router)#neighbor 6.6.6.6 remote-as 300
```

In this configuration, the neighbor 5.5.5.4 has an eBGP connection to confederation 300.

```
#configure terminal
(config)#router bgp 500
(config-router)#neighbor 5.5.5.4 remote-as 300
```

bgp config-type

Use this command to set the BGP configuration to the `standard` type. After setting the configuration to the `standard` type, use the neighbor send-community command to send out BGP community attributes. The `zebos` configuration type is the default and requires no specific configuration for sending out BGP standard community and extended community attributes.

For the `standard` type, the `no synchronization` command is always shown in the configuration, whereas for the `zebos` type, this command is the default.

Use the no parameter with this command to remove this configuration.

Command Syntax

```
bgp config-type (standard|zebos)
no bgp config-type
```

Parameters

`standard`	Standard style configuration
`zebos`	OcNOS style configuration

Default

The default configuration type is: bgp config-type zebos

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp config-type standard
```

bgp dampening

Use this command to enable BGP route dampening and set various parameters. Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the `suppress` limit the advertisement of the route is suppressed. This penalty is decayed according to the configured `half time` value. Once the penalty is lower than the `reuse` limit, the route advertisement is un-suppressed. The dampening information is purged from the router once the penalty becomes less than half of the `reuse` limit.

Use the `no` parameter with this command to unset BGP dampening parameters.

Command Syntax

```
bgp dampening
bgp dampening <1-45>
bgp dampening <1-45> <1-20000> <1-20000> <1-255>
bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>
bgp dampening route-map WORD
no bgp dampening
no bgp dampening <1-45>
no bgp dampening <1-45> <1-20000> <1-20000> <1-255>
no bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>
no bgp dampening route-map
no bgp dampening route-map WORD
```

Parameters

`<1-45>`	Reachability half-life time for the penalty in minutes. The time for the penalty to decrease to one-half of its current value.
`<1-20000>`	Value to start reusing a route. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
`<1-20000>`	Value to start suppressing a route. When the penalty for a route exceeds the suppress value, the route is suppressed
`<1-255>`	Maximum duration to suppress a stable route in minutes.
`<1-45>`	Un-reachability half-life time for the penalty in minutes.
`route-map`	Route map to specify criteria for dampening.
`WORD`	Route-map name.

Defaults

The default reachability half-life is 15 minutes.

The default reuse limit is 750.

The default suppress limit is 2000.

The default max-suppress value is 4 times the half-life time, or 60 minutes.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 11
(config-router)#bgp dampening 20 800 2500 80 25
```

bgp default ipv4-unicast

Use this command to configure BGP defaults and activate IPv4-unicast for a peer by default. This affects the BGP global configuration.

Use the no parameter with this command to disable the default behavior of the BGP routing process of exchanging IPv4 addressing information with BGP neighbor routers.

Command Syntax

```
bgp default ipv4-unicast
no bgp default ipv4-unicast
```

Parameters

None

Default

IPv4 unicast is the default BGP behavior.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp default ipv4-unicast
```

bgp default local-preference

Use this command to change the default local preference value.Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. The preference is sent to all routers and access servers in the local autonomous system.

Use the no parameter with this command to revert to the default value for local preference.

Command Syntax

```
bgp default local-preference <0-4294967295>
no bgp default local-preference
no bgp default local-preference <0-4294967295>
```

Parameter

`<0-4294967295>` Local preference value

Default

By default, local preference value is 100

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp default local-preference 2345555
```

bgp deterministic-med

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

For a correct comparison result, enable this command on all routers in a local AS. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value. Based on this comparison, the best path is then chosen. This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp always-compare-med command.

When the bgp deterministic-med command is enabled, routes from the same AS are grouped together, and the best routes of each group are compared. If the BGP table showed:

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP would have a group of Route1 and a second group of Route2 and Route3 (the same ASs). The best of each group is compared. Route1 is the best of its group because it is the only route from AS 200. Route1 is compared to the Route2, the best of group AS 400 (the lower MED). Since the two routes are not from the same AS, the MED is not considered in the comparison. The external BGP route is preferred over the internal BGP route, making Route3 the best route; the preferred route would be different if `always-compare-med` command is enabled (See `always-compare-med` command).

Use the `no` parameter with this command to disallow this setting.

Command Syntax

```
bgp deterministic-med
```

```
no bgp deterministic-med
```

Parameters

None

Default

By default, bgp deterministic med is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp deterministic-med

(config)#router bgp 100
(config-router)#no bgp deterministic-med
```

bgp enforce-first-as

Use this command to enforce the first AS for eBGP routes. This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Using the no parameter with this command to disable this feature.

Command Syntax

```
bgp enforce-first-as
no bgp enforce-first-as
```

Parameters

None

Default

By default, enforce-first-as is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp enforce-first-as

(config)#router bgp 100
(config-router)#no bgp enforce-first-as
```

bgp extended-asn-cap

Use this command to configure a BGP router to send 4-octet ASN capabilities. If attempting to change the AS capability from 2 to 4 or 4 to 2, a prompt occurs to remove the VRF configuration (if it exists), and reconfiguration is required, because the route distinguisher (RD) configuration would have been created with the current (2 octet or 4 octet) capability, and must be reconfigured before attempting to change the capability.

While loading from a saved configuration with AS4 capability and BGP VRF configuration, the capability will not be changed because of the above described reason.

Use the no parameter with this command to prevent a BGP router from sending 4-octet ASN capabilities.

Command Syntax

```
bgp extended-asn-cap
no bgp extended-asn-cap
```

Parameters

None

Default

By default, the bgp extended ASN capability and Four-octet capabilities are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp extended-asn-cap
```

bgp fast-external-failover

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down.

Use the no parameter with this command to disable this feature.

Command Syntax

```
bgp fast-external-failover
no bgp fast-external-failover
```

Parameters

None

Default

By default, fast-external failover is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp fast-external-failover
```

bgp log-neighbor-changes

Use this command to enable logging of status change messages without turning on debug bgp commands. OcNOS has many logging services for neighbor status, including `debug bgp fsm` and `debug bgp events`. However, these commands cause system performance degradation. If you need to log neighbor status changes only, IP Infusion Inc. recommends turning off all debug commands and using the `bgp log-neighbor-changes` command instead. A sample output of the log is:

```
%Protocol-Severity-Events: Message-text
```

A sample output of the log for an `interface down` event is:

```
%BGP-5-ADJCHANGE: neighbor 10.10.0.24 Down Interface flap
```

This command logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

Parameters

None

Default

By default, bgp log neighbor changes is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#router bgp 100
(config-router)#bgp log-neighbor-changes
```

bgp multiple-instance

Use this command to enable BGP multiple instance support.

Use the no parameter with this command to disable this function.

Note: The `no bgp multiple-instance` command is not valid when any BGP instances are present.

Command Syntax

```
bgp multiple-instance (allow-same-peer|)
no bgp multiple-instance (allow-same-peer|)
```

Parameters

`allow-same-peer`

Allow the same peer in multiple instances

Default

By default, there is no multiple-instance support in BGP

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the use of the `bgp multiple-instance` command allowing the configuration of two instances.

```
(config)#bgp multiple-instance

(config)#quit
#show running-config

Current configuration:
hostname OcNOS
password zebra
log stdout
!
debug bgp
debug bgp events
debug bgp updates
debug bgp fsm
!
bgp multiple-instance
!
router bgp 11
 bgp router-id 10.10.10.50
 neighbor 10.10.10.51 remote-as 11
!
```

bgp nexthop-trigger delay

Use this command to set the delay time for nexthop address tracking. This command configures the delay interval between routing table walks for nexthop delay tracking, after which BGP does a routing table scan on receiving a nexthop change trigger from NSM. The time period determines how long BGP waits before it walks the full BGP table to determine which prefixes are affected by the nexthop changes, after it receives the trigger from NSM about one or more nexthop changes.

Use the no parameter with this command to reset the timer value to the default value.

Command Syntax

```
bgp nexthop-trigger delay <1-100>
no bgp nexthop-trigger delay
```

Parameter

<1-100>	Nexthop trigger delay interval in seconds

Default

By default, nexthop-trigger delay time is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger delay 6

#configure terminal
(config)#no bgp nexthop-trigger delay
```

bgp nexthop-trigger enable

Use this command to enable nexthop address tracking. Nexthop address tracking is an event-driven notification system that monitors the status of routes installed in the Routing Information Base (RIB) and reports nexthop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the BGP process. This improves the overall BGP convergence time, by allowing BGP to respond rapidly to nexthop changes for routes installed in the RIB.

If nexthop tracking is enabled after certain routes are learned, the registration of all nexthops for selected BGP routes is done after the nexthop tracking feature is enabled. If nexthop tracking is disabled, and if there are still some selected BGP routes, BGP de-registers the nexthops of all selected BGP routes from NSM.

Use the `no` parameter with this command to disable this feature. If the `no` command is given when nexthop tracking is in the process of execution, an error appears and nexthop tracking is not disabled. However, if the nexthop tracking timer is running at the time of negation, the nexthop tracking timer is stopped, and nexthop tracking is disabled.

Command Syntax

```
bgp nexthop-trigger enable
```

```
no bgp nexthop-trigger enable
```

Parameters

None

Default

By default, nexthop address tracking is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger enable
```

bgp rfc1771-path-select

Use this command to set RFC 1771 compatible path selection.

Use the no parameter with this command to revert this setting.

Command Syntax

```
bgp rfc1771-path-select
no bgp rfc1771-path-select
```

Parameters

None

Default

Standard compatible path selection mechanism.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-path-select
```

bgp rfc1771-strict

Use this command to set the origin path attribute to “IGP” when the origin is a protocol such as OSPF or ISIS as specified in RFC 1771. Otherwise, the origin is always set to “incomplete” which is the industry standard.

Use the no parameter with this command to revert this setting.

Command Syntax

```
bgp rfc1771-strict
no bgp rfc1771-strict
```

Parameters

None

Default

By default, bgp rfc1771 strict is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-strict
```

bgp router-id

Use this command to manually configure a fixed router ID as a BGP router identifier. When this command is used to configure a fixed router ID, the current router identifier is overridden and the peers are reset.

Use the no parameter with this command to remove a manually configured fixed router ID.

Command Syntax

```
bgp router-id A.B.C.D
no bgp router-id
no bgp router-id A.B.C.D
```

Parameter

A.B.C.D	Router ID in an IPv4 address format

Default

Once the BGP router-id is elected, it may be re-elected in the following cases:

a. When an explicit BGP router-id is configured/un-configured

b. When the router's (global) router-id is set/unset (holds true when (a) is not applicable),

c. When the BGP process is cleared (holds true when both (a) & (b) are not applicable and the IP address(es) on the active interfaces are updated, which may result in a change in the router's router-id).

If no loopback interface is configured, the highest IP address is the BGP router-id.

When a loopback interface is configured, the BGP router-id is set to the IP address of the loopback interface.

Note: IP Infusion Inc. recommends that you always configure a router identifier to avoid unpredictable behavior if the address of a loopback interface changes.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp router-id 10.1.2.7

(config)#router bgp 100
(config-router)#no bgp router-id 10.1.2.7
```

bgp scan-time

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database. To disable BGP scanning, set the scan-time interval to 0 seconds.

Use the no parameter with this command to disable this function.

Note: When BGP scan timer is disabled, existing routes in BGP RIB will not be updated with the updated redistributed configuration.

Command Syntax

```
bgp scan-time <0-60>
no bgp scan-time
no bgp scan-time <0-60>
```

Parameter

<0-60>	Scanning interval in seconds

Default

By default, scan-time interval is 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp scan-time 10
```

bgp table-map

Use this command to enable or disable suppression/modification of incoming BGP updates to IP RIB/FIB table installation.

In a dedicated route reflector, all the routes it receives may not be required to be stored or only few selected routes need to be stored, because it may not lie in the data path.

Table maps are particularly useful to attain this restriction. Table-map command can be used in two ways:

- When a simple table-map command is given, the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option ‘filter’ is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Use this command in Router mode to set the table map rule for all address families. Use this command in Address Family mode to set the table map rule per an IPv4 or IPv6 family.

Use the no parameter with this command to remove the table-map rule.

Command Syntax

```
table-map WORD (|filter)
```

Parameter

WORD	Specify the route-map name to apply.
filter	Filer the routes. If present, the incoming routes are pruned as per the rule specified in route-map-name. If not, it is used to alter the incoming packet information.

Default

All BGP routes will be downloaded to IP RIB

Command Mode

Router mode, Address Family IPv4 mode, and Address Family IPv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the table-map command without a filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#table-map abc
```

The following example shows how to set the table-map command with a filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#table-map abc filter
```

The following example shows how to set the table-map command without a filter for BGP for the IPv6 address family.

```
(config)#router bgp 100
(config-router)#address-family ipv6
(config-router-af)#table-map abc
```

The following example shows how to set the table-map command with a filter for BGP for the IPv6 address family.

```
(config)#router bgp 100
(config-router)#address-family ipv6
(config-router-af)#table-map abc filter
```

clear bgp (A.B.C.D|X:X::X:X)

Use this command to reset a BGP neighbor address.

Command Syntax

```
clear bgp (A.B.C.D|X:X::X:X)
clear bgp (A.B.C.D|X:X::X:X) in
clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
clear bgp (A.B.C.D|X:X::X:X) out
```

Parameters

`A.B.C.D`	IPv4 neighbor address.
`X:X::X:X`	IPv6 neighbor address.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 3.3.3.3
```

clear bgp *

Use this command to reset the BGP connection for all peers.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp *
clear bgp * in
clear bgp * in prefix-filter
clear bgp * out
clear bgp * soft
clear bgp * soft in
clear bgp * soft out
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * out
clear ip bgp * soft
clear ip bgp * soft in
clear ip bgp * soft out
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
clear ip bgp * ipv4 (unicast|multicast) soft in
clear ip bgp * ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Incoming advertised routes should be cleared.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp *
#clear ip bgp * ipv4 unicast in prefix-filter
```

clear bgp <1-4294967295>

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp <1-4294967295>
clear bgp <1-4294967295> in
clear bgp <1-4294967295> in prefix-filter
clear bgp <1-4294967295> out
clear bgp <1-4294967295> soft
clear bgp <1-4294967295> soft in
clear bgp <1-4294967295> soft out
clear ip bgp <1-4294967295>
clear ip bgp <1-4294967295> in
clear ip bgp <1-4294967295> in prefix-filter
clear ip bgp <1-4294967295> out
clear ip bgp <1-4294967295> soft
clear ip bgp <1-4294967295> soft in
clear ip bgp <1-4294967295> soft out
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in prefix-filter
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) out
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft in
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.

	Clear incoming advertised routes.
`in`	Clear incoming advertised routes.
`prefix-filter`	
	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp 4294967277
#clear ip bgp 4294967277
```

clear bgp dampening

Use this command to reset BGP route flap dampening information.

Command Syntax

```
clear bgp ipv4 (unicast|multicast) dampening
clear bgp ipv4 (unicast|multicast) dampening A.B.C.D/M
clear ip bgp dampening
clear ip bgp dampening A.B.C.D/M
clear ip bgp ipv4 (unicast|multicast) dampening
clear ip bgp ipv4 (unicast|multicast) dampening A.B.C.D/M
```

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp dampening 10.10.0.121/24
#clear ip bgp ipv4 unicast dampening
```

clear bgp external

Use this command to reset the BGP connection for all external peers.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp external
clear bgp external in
clear bgp external in prefix-filter
clear bgp external out
clear bgp external soft
clear bgp external soft in
clear bgp external soft out
clear ip bgp external
clear ip bgp external in
clear ip bgp external in prefix-filter
clear ip bgp external out
clear ip bgp external soft
clear ip bgp external soft in
clear ip bgp external soft out
clear ip bgp external ipv4 (unicast|multicast) in
clear ip bgp external ipv4 (unicast|multicast) in prefix-filter
clear ip bgp external ipv4 (unicast|multicast) out
clear ip bgp external ipv4 (unicast|multicast) soft
clear ip bgp external ipv4 (unicast|multicast) soft in
clear ip bgp external ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip bgp external
```

clear bgp flap-statistics

Use this command to reset BGP flap statistics.

Command Syntax

```
clear bgp ipv4 (unicast|multicast) flap-statistics
clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default |
  VRFNAME )
clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M
clear ip bgp flap-statistics
clear ip bgp flap-statistics A.B.C.D/M
clear ip bgp ipv4 (unicast|multicast) flap-statistics
clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default
  | VRFNAME )
clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M
```

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`VRFNAME`	VPN routing or forwarding instance name
`all`	All VRF's
`default`	Default VRF

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp flap-statistics
#clear ip bgp ipv4 unicast flap-statistics
```

clear bgp peer-group

Use this command to reset the BGP connection for all members of a peer group.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp peer-group WORD
clear bgp peer-group WORD in
clear bgp peer-group WORD in prefix-filter
clear bgp peer-group WORD out
clear bgp peer-group WORD soft
clear bgp peer-group WORD soft in
clear bgp peer-group WORD soft out
clear ip bgp peer-group WORD
clear ip bgp peer-group WORD in
clear ip bgp peer-group WORD in prefix-filter
clear ip bgp peer-group WORD out
clear ip bgp peer-group WORD soft
clear ip bgp peer-group WORD soft in
clear ip bgp peer-group WORD soft out
clear ip bgp peer-group WORD ipv4 (unicast|multicast) in
clear ip bgp peer-group WORD ipv4 (unicast|multicast) in prefix-filter
clear ip bgp peer-group WORD ipv4 (unicast|multicast) out
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft in
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft out
```

Parameters

`WORD`	BGP peer-group name.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.

	`unicast`	Unicast prefixes.
		Clear incoming advertised routes.
	`in`	Clear incoming advertised routes.
	`prefix-filter`	
		Push out prefix-list ORF and do inbound soft reconfig.
	`out`	Clear outgoing advertised routes.
	`soft`	Clear both incoming and outgoing routes.
	`in`	Soft reconfig inbound update.
	`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp peer-group P1
```

clear bgp statistics

Use this command to reset all BGP statistics.

Command Syntax

```
clear bgp statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp statistics
```

clear bgp view

Use this command to reset all peers in a BGP view.

Command Syntax

```
clear bgp view WORD *
clear bgp view WORD * soft
clear bgp view WORD * soft in
clear bgp view WORD * soft out
clear ip bgp view WORD *
clear ip bgp view WORD * in prefix-filter
clear ip bgp view WORD * soft
clear ip bgp view WORD * soft in
clear ip bgp view WORD * soft out
clear ip bgp view WORD * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp view WORD * ipv4 (unicast|multicast) soft
clear ip bgp view WORD * ipv4 (unicast|multicast) soft in
clear ip bgp view WORD * ipv4 (unicast|multicast) soft out
```

Parameters

`WORD`	BGP peer group name.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp view myview *
```

clear ip bgp A.B.C.D

Use this command to reset an IPv4 BGP neighbor address.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp A.B.C.D in
clear ip bgp A.B.C.D in prefix-filter
clear ip bgp A.B.C.D out
clear ip bgp A.B.C.D soft
clear ip bgp A.B.C.D soft in
clear ip bgp A.B.C.D soft out
clear ip bgp A.B.C.D ipv4 (unicast|multicast) in
clear ip bgp A.B.C.D ipv4 (unicast|multicast) in prefix-filter
clear ip bgp A.B.C.D ipv4 (unicast|multicast) out
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft in
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 in
```

clear ip bgp A.B.C.D vrf

Use this command to reset the VPN Routing/Forwarding (VRF) instance for a peer address.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp A.B.C.D vrf WORD
clear ip bgp A.B.C.D vrf WORD in
clear ip bgp A.B.C.D vrf WORD out
clear ip bgp A.B.C.D vrf WORD soft
clear ip bgp A.B.C.D vrf WORD soft in
clear ip bgp A.B.C.D vrf WORD soft out
```

Parameters

`A.B.C.D`	IPv4 address
`WORD`	VPN routing/forwarding instance name
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 vrf
```

clear ip bgp A.B.C.D ipv4 labeled-unicast

Use this command to soft reset an IPv4 Labeled-unicast BGP neighbor.

Command Syntax

```
clear ip bgp A.B.C.D ipv4 labeled-unicast soft
clear ip bgp A.B.C.D ipv4 labeled-unicast soft in
clear ip bgp A.B.C.D ipv4 labeled-unicast soft out
```

Parameters

`A.B.C.D`	BGP neighbor address
`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp A.B.C.D ipv4 labeled-unicast soft in
```

clear ip bgp peer-group WORD ipv4 labeled-unicast

Use this command to soft reset an peer-group of ipv4 labeled-unicast peer members.

Command Syntax

```
clear ip bgp peer-group WORD ipv4 labeled-unicast soft
clear ip bgp peer-group WORD ipv4 labeled-unicast soft in
clear ip bgp peer-group WORD ipv4 labeled-unicast soft out
```

Parameters

`WORD`	Peer-group name
`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp peer-group LU_GROUP ipv4 labeled-unicast soft in
```

clear ip bgp * ipv4 labeled-unicast

Use this command to soft reset all IPv4 Labeled-unicast BGP neighbors.

Command Syntax

```
clear ip bgp * ipv4 labeled-unicast soft
clear ip bgp * ipv4 labeled-unicast soft in
clear ip bgp * ipv4 labeled-unicast soft out
```

Parameters

`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp * ipv4 labeled-unicast soft in
```

clear ip bgp table-map

Use this command to apply the modified table map or route map rules to the BGP routes in the existing IP routing table.

Command Syntax

```
clear ip bgp table-map (vrf (VRFNAME|all|default))
clear ip bgp ipv4 (unicast | multicast) table-map(vrf (VRFNAME|all|default))
```

Parameters

`vrf`	Select a VPN Routing/Forwarding Instance.
`VRFNAME`	Specify a VPN Routing/Forwarding instance name.
`all`	Select all VRFs.
`default`	Select default VRFs.
`unicast`	Unicast prefixes.
`multicast`	Multicast prefixes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp table-map vrf all
```

debug bgp

Use this command to enable all BGP troubleshooting functions. Use this command without any parameters to turn on normal bgp debug information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug bgp (all|)
debug bgp bfd
debug bgp dampening
debug bgp events
debug bgp filters
debug bgp fsm
debug bgp keepalives
debug bgp mpls
debug bgp nht
debug bgp nsm
debug bgp updates
debug bgp updates (in|out)
debug bgp vpls
no debug bgp (all|)
no debug bgp bfd
no debug bgp events
no debug bgp dampening
no debug bgp filters
no debug bgp fsm
no debug bgp keepalives
no debug bgp mpls
no debug bgp nht
no debug bgp nsm
no debug bgp updates
no debug bgp vpls
undebug bgp (all|)
undebug bgp bfd
undebug bgp dampening
undebug bgp events
undebug bgp filters
undebug bgp fsm
undebug bgp keepalives
```

```
undebug bgp mpls
undebug bgp nht
undebug bgp nsm
undebug bgp updates
undebug bgp vpls
```

Parameters

`all`	Used only with the no form; turns off all debugging for BGP
`bfd`	Enable debugging for BGP Bidirectional Forwarding Detection
`dampening`	Enable debugging for BGP dampening
`events`	Enable debugging for BGP events
`filters`	Enable debugging for BGP filters
`fsm`	Enable debugging for BGP Finite State Machine (FSM)
`keepalives`	Enable debugging for BGP keepalives
`mpls`	Enable debugging for BGP Multiprotocol Label Switching (MPLS)
`nht`	Enable debugging for BGP NHT
`nsm`	Enable debugging for NSM messages
`updates`	Enable debugging for BGP updates
`in`	Debug inbound updates
`out`	Debug outbound updates
`vpls`	Enable debugging for BGP Virtual Private LAN Service (VPLS)

Command Mode

Privileged Exec mode and Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug bgp
#debug bgp events
```

distance bgp

Use this command to define an administrative distance. A distance is a rating of trustworthiness of a router. The higher the distance the lower the trust rating. Administrative distances can be set for external, internal and local routes. External paths are routes learned from a neighbor outside of the AS. Internal routes are routes learned from another router within the same AS. Local routes are for a router that is redistributed from another process.

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing. Use this command in Router mode to set the administrative distance for all address families. Use this command in Address Family mode to set the administrative distance per an IPv4 family.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance bgp <1-255> <1-255> <1-255>
no distance bgp
no distance bgp <1-255> <1-255> <1-255>
```

Parameters

<1-255>	Distance for BGP external routes
<1-255>	Distance for BGP internal routes
<1-255>	Distance for BGP local routes

Command Mode

Router mode, Address Family IPv4 mode

Defaults

Default distance for external routes is 20.

Default distance for internal routes is 200.

Default distance for local routes is 200.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the administrative distance for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#distance bgp 34 23 15
```

exit-address-family

Use this command to exit address-family mode.

For information on how to enter address family mode, see address-family.

Command Syntax

```
exit-address-family
```

Parameters

None

Default

Not applicable

Command Mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 multicast
(config-router-af)#exit-address-family
(config-router)#
```

ip as-path access-list

Use this command to define a BGP Autonomous System (AS) path access list. A named community list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the permit or deny condition applies. Use this command to define the BGP access list globally; use the neighbor router configuration command to apply a specific access list.

Use the no parameter with this command to disable use of the access list.

Command Syntax

```
ip as-path access-list WORD (deny|permit) LINE
no ip as-path access-list WORD
no ip as-path access-list WORD (deny|permit) LINE
```

Parameters

`WORD`	Access list name
`deny`	Reject packets
`permit`	Forward packets
`LINE`	An ordered list as a regular expression

Default

Not applicable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip as-path access-list mylist deny ^65535$
```

ip community-list <1-99>

Use this command to specify a standard community list (1 to 99) that specifies BGP community attributes.

Use the no parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list <1-99> (deny|permit)
ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
no ip community-list <1-99> (deny|permit)
no ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 55 permit 7675:80 7675:90

(config)#no ip community-list 55 permit 7675:80 7675:90
```

ip community-list <100-500>

Use this command to specify an expanded community list (100 to 500) that specifies BGP community attributes.

Use the no parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list <100-500> (deny|permit)
ip community-list <100-500> (deny|permit) LINE
no ip community-list <100-500>
no ip community-list <100-500> (deny|permit) LINE
```

Parameters

deny	Reject community
permit	Accept community
LINE	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 225 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```

ip community-list expanded

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long.

There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the community attributes with regular expressions.Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list expanded WORD (deny|permit) LINE
no ip community-list expanded WORD
no ip community-list expanded WORD (deny|permit) LINE
```

Parameters

`WORD`	Community list name
`deny`	Reject community
`permit`	Accept community
`LINE`	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 125 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```

ip community-list standard

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long. There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format without regular expressions. The expanded community-list defines the community attributes with regular expressions.

Use this command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Use the `no` parameter with this command to delete the standard community-list entry.

Command Syntax

```
ip community-list standard WORD (deny|permit)
ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
no ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

`WORD`	Community list name
`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list standard CLIST permit 7675:80 7675:90 no-export
(config)#ip community-list 34 permit 5675:50 no-advertise
```

ip community-list WORD

Use the community-list commands to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. There are two kinds of community-lists: the expanded and standard. The `standard community-list` defines the community attributes in a specified format and not with regular expressions. The `expanded community-list` defines the community attributes with regular expressions.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list WORD (deny|permit)
ip community-list WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-
  export]
no ip community-list WORD
no ip community-list WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-
  export]
```

Parameters

`WORD`	Community list name
`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list mylist permit 7675:80 7675:90

(config)#no ip community-list mylist permit 7675:80 7675:90
```

ip extcommunity-list <1-99>

Use this command to create an entry for a standard extended community list.

Use the no parameter with this command to delete the community-list entry.

Command Syntax

```
ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo)
no ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo)
```

Parameters

deny	Reject community
permit	Accept community
LINE	One of the following:
rt	Route target extended community in aa:nn or IPaddr:nn format
soo	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 3 permit rt 10.10.23.123:67

(config)#ip extcommunity-list 25 deny soo 1465:22
```

ip extcommunity-list <100-500>

Use this command to create an extended community list.

Use the no parameter with this command to delete the community-list entry.

Command Syntax

```
ip extcommunity-list <100-500> (deny|permit) LINE
no ip extcommunity-list <100-500> (deny|permit) LINE
```

Parameters

`<100-500>`	Extended community list number (expanded)
`deny`	Reject the community
`permit`	Accept the community
`LINE`	Any regular expression:

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 125 permit 4567:335

(config)#ip extcommunity-list 231 deny *.
```

ip extcommunity-list expanded

Use this command to create an expanded community list.

Use the no parameter with this command to delete the expanded community-list entry.

Command Syntax

```
ip extcommunity-list expanded WORD
ip extcommunity-list expanded WORD (deny|permit) LINE
no ip extcommunity-list expanded WORD
no ip extcommunity-list expanded WORD (deny|permit) LINE
```

Parameters

WORD	Expanded community list name
deny	Reject the community
permit	Accept the community
LINE	One of the following:
rt	Route target extended community in aa:nn or IPaddr:nn format
soo	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 125 permit 4567335
(config)#ip extcommunity-list expanded CLIST permit .*
```

ip extcommunity-list standard

Use this command to create and delete a standard extended-community list. The extended community attribute is 8 bytes in 2 formats. The sub-type can be route target (`rt`) or site of origin (`soo`). Thus, the sub-type of each community must be specified when creating the extended community list. Regarding the formats, an extended community is based on a 6-byte value. These 6-bytes are represented in 4-btye:2-byte format, and may be entered in one of the following forms:

- Format 1, aa.nn: The 16-bit value of the AS (aa) number is represented in the higher-order 4-bytes. If the extended ASN capability is enabled, the AS number is represented using higher-order 4-bytes. The nn assigned value is represented in the low-order 2-bytes in both cases.
- Format 2, IPaddr:nn: In this format, the higher-order 4-bytes are used to represent the IP address, and the low-order 2-bytes are used to represent the assigned value.

Use the `no` parameter with this command to delete the extended-community-list entry.

Command Syntax

```
ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn)
no ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn)
```

Parameters

`WORD`	Extended community list name
`deny`	Reject the community
`permit`	Accept the community
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list standard 36 permit rt 5675:50
(config)#ip extcommunity-list standard CLIST permit soo 10.10.32.15:70
```

match ip peer

Use this command to apply policies based on the route source of which the BGP TCP/IP session formed using an IPv4 address in the update message.

Use the no parameter with this command to disable this function.

Command Syntax

```
match ip peer (<1-199>|<1300-2699>|WORD)
no match ip peer (<1-199>|<1300-2699>|WORD)
```

Parameters

<1-199>	IP access-list number
<1300-2699>	IP access-list number (expanded range)
WORD	Access-list name

Default

By default, import bgp route is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map in-A permit 10
(route-map)#match ip peer 1
```

max-paths

Use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. You can install multiple BGP paths to the same destination to balance the load on the forwarding path.

Use the no parameter with this command to disable this feature.

Command Syntax

```
max-paths (ebgp|ibgp|) <2-64>
no max-paths ebgp (<2-64>|)
no max-paths ibgp (<2-64>|)
```

Parameters

ebgp	eBGP ECMP session
ibgp	iBGP ECMP session
<2-64>	Number of routes

Default

Available for the default BGP instance and for IPv4 and IPv6 unicast addresses

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures 7 routes for ECMP for iBGP.

```
#configure terminal
(config)#router bgp 11
(config-router)#max-paths ibgp 7
```

neighbor activate

Use this command to enable the exchange of specific address family routes with a neighboring router. After a TCP connection is opened with a neighboring router, use this command to enable or disable the exchange of address family information. To enable the exchange of multicast and VPNv4 address prefix types, activate neighbors using this command in address family mode.

Use the no parameter with this command to disable exchange of information with a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) activate
no neighbor (A.B.C.D|X:X::X:X|WORD) activate
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

A neighbor under address-family IPv4 is activated by default. For all other address-families, use this command to enable a neighbor to exchange routing information of a specific address-family with a neighbor.

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 activate

(config)#router bgp 100
(config-router)#neighbor 10.10.20.1 remote-as 100
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 10.10.20.1 activate
```

neighbor additional-paths

Use this command to enable neighbour BGP add-path.

Use the no parameter with this command to disable neighbour BGP add-path.

Command Syntax

```
neighbor A.B.C.D additional-paths (send|receive|send-receive|disable)
no neighbor A.B.C.D additional-paths (send|receive|send-receive|disable)
```

Parameters

`send`	Send additional paths to neighbors
`receive`	Receive additional paths from neighbors
`send-receive`	Send and Receive additional paths from neighbors
`disable`	Disable additional paths

Default

By default additional-path is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#neighbor 1.1.1.2 additional-paths send

(config-router)#no neighbor 1.1.1.2 additional-paths send
```

neighbor advertise additional-paths

Use this command to enable BGP add-path at neighbor level.

Use the no parameter with this command to disable BGP add-path at neighbor level.

Command Syntax

```
neighbor A.B.C.D advertise additional-paths (all|best <2-3>)
no neighbor A.B.C.D advertise additional-paths (all|best <2-3>)
```

Parameters

all	Select all available paths
best	Select best N paths
<2-3>	Number of best paths in additional paths to be selected

Default

By default, neighbor advertise additional path is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#neighbor  1.1.1.2 advertise additional-paths all

(config-router)#no neighbor  1.1.1.2 advertise additional-paths all
```

neighbor advertisement-interval

Use this command to set a minimum interval between the sending of BGP routing updates. To reduce the flapping of routes, set a minimum advertisement interval so that the BGP routing updates are sent only per interval seconds. BGP dampening can also be used to control the effects of flapping routes.

Use the no parameter with this command to set the interval time to default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval
no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<0-65535>	Advertisement interval value in seconds

Default

By default, neighbor value for ebgp peer is 30 seconds and IBGP peer is 5 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.3 advertisement-interval 45
```

neighbor allowas-in

Use this command to advertise prefixes (routes) even when the source of the prefixes is from the same Autonomous System (AS) number.

Use this command in a scenario where two routers at different locations use the same Autonomous System number and are connected via an ISP. Once prefixes arrive from one branch at the ISP, they are tagged with the customer's AS number. By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router uses the same AS number. Use this command to advertise the prefixes at the other side. Control the number of times an AS number is advertised by specifying a number.

In a hub and spoke configuration in a VPN, a PE (Provider Edge) router advertises all prefixes containing duplicate AS numbers. Use this command to configure two VRFs on each PE router to receive and advertise prefixes. One of the VRFs receives prefixes with AS numbers from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with AS numbers from the CE (Customer Edge) router and advertises them to all PE routers in the hub and spoke configuration.

Use the `no` parameter with this command to reset to default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in
neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in <1-10>
no neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in
```

Parameters

`A.B.C.D`	IPv4 neighbor address.
`X:X::X:X`	IPv6 neighbor address.
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-10>`	Number of times to allow the advertisement of an AS number.

Default

By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router uses the same AS number. The default number of local AS is 3.

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.3 allowas-in 4

#configure terminal
(config)#router bgp 7657
```

```
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 allowas-in 3

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 allowas-in 3
```

neighbor as-origination-interval

Use this command to set the minimum interval between sending of AS-origination routing updates.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval
no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-65535>	AS origination interval in seconds

Default

By default, neighbor as origination interval is 15 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.75 as-origination-interval 555
```

neighbor attribute-unchanged

Use this command to advertise unchanged BGP attributes to the specified neighbor.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged ({ as-path|next-hop|med }|)
no neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged (({ as-path|next-hop|
  med }|)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`as-path`	AS path attribute
`next-hop`	Nexthop attribute
`med`	Multi-exit discriminator attribute

Default

By default, the neighbor attribute-unchanged is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.75 attribute-unchanged as-path med
```

neighbor capability dynamic

Use this command to enable the dynamic capability for a specific peer. This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.

Use the no parameter with this command to disable the dynamic capability.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic
no neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor capability dynamic is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 capability dynamic
```

neighbor capability orf prefix-list

Use this command to enable Outbound Router Filtering (ORF) and advertise the ORF capability to its neighbors. The ORFs send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The two routers exchange updates to maintain the ORF for each router:

- The local router advertises the ORF capability in `send` mode.
- The remote router receives the ORF capability in `receive` mode, applying the filter as outbound policy.

Only an individual router or a peer group can be configured to be in `receive` or `send` mode. A peer-group member cannot be configured to be in `receive` or `send` mode.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send)
no neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	The local router can send ORF entries to its peer, as well as receive ORF entries from its peer.
`receive`	The local router is willing to receive ORF entries from its peer
`send`	The local router is willing to send ORF entries to its peer

Default

By default, the orf prefix-list is disabled

Command Mode

Router mode and Address Family (IPv4 unicast, IPv4 multicast, IPv6) mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.5 capability orf prefix-list both
(config-router)#neighbor effe:2897::0003:3ed5 capability orf prefix-list
receive
```

neighbor capability route-refresh

'Route Refresh Capability', which would allow the dynamic exchange of route refresh request between BGP speakers and subsequent re-advertisement of the respective Adj-RIB-Out.

Default

By default, neighbor capability route refresh is enabled and it can not be disabled.

neighbor collide-established

Use this command to include a neighbor already in an established state for conflict resolution when a TCP connection collision is detected. This command is not required for most network deployments, so users should only use this command when required.

Note: The associated functionality of including an “established” neighbor into TCP connection collision conflict resolution is automatically enabled when a neighbor is configured for BGP graceful-restart.

Use the no option with this command to turn this feature off.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) collide-established
no neighbor (A.B.C.D|X:X::X:X|WORD) collide-established
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor collide is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 collide-established
```

neighbor connection-retry-time

Use this command to set the connection retry time for a specific BGP neighbor.

Use the no parameter with this command to clear the connection retry time for a specific BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time <1-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time
no neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time <1-65535>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-65535>	Connection retry time in seconds

Default

By default, connection retry time is 120 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 connection-retry-time 125
```

neighbor default-originate

Use this command to allow a BGP local router to send the default route 0.0.0.0 to a neighbor to use as a default route. This command can be used with standard or extended access lists.

Use the no parameter with this command to send no route as a default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) default-originate
neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate
no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Route map name

Default

By default, neighbor default originate is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 default-originate route-map myroute
```

neighbor description

Use this command to associate a description with a neighbor. This command helps to identify a neighbor quickly. This command is useful for an ISP that has multiple neighbor relationships.

Use the no parameter with this command to remove the description.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) description LINE
no neighbor (A.B.C.D|X:X::X:X|WORD) description
no neighbor (A.B.C.D|X:X::X:X|WORD) description LINE
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
LINE	Neighbor description (up to 80 characters)

Default

By default, the neighbor description is disabled

Command Mode

Router mode and Address Family

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 description Backup router for sales

(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 description Bank of America

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 description Bank of America
```

neighbor disallow-infinite-holdtime

Use this command to disallow configuration of infinite hold-time. This command enables the local BGP speaker to reject a hold-time of “0” seconds from a peer (during exchange of open messages) or a user (during configuration).

The no form of this command allows the BGP speaker to accept a hold-time of “0” from a peer or during configuration.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime
no neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor disallow infinite holdtime is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config-router)#neighbor 10.11.4.26 disallow-infinite-holdtime
(config-router)#neighbor 3ffe::45 disallow-infinite-holdtime
```

neighbor distribute-list

Use this command to filter route updates from a particular BGP neighbor. Use only one distribute list per BGP neighbor.

Use the no parameter with this command to remove an entry.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD)
  (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD)
  (in|out)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-199>	IP access-list number
<1300-2699>	IP access-list number (expanded-range)
WORD	Access-list name
in	Filter incoming advertised routes
out	Filter outgoing advertised routes

Default

By default, neighbor distribute list is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 distribute-list mylist out
```

neighbor dont-capability-negotiate

Use this command to disable capability negotiation. This command is used to allow compatibility with older BGP versions that have no capability parameters used in open messages between peers.

Use the no parameter with this command to enable capability negotiation.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate
no neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, capability negotiation is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 dont-capability-negotiate
```

neighbor ebgp-multihop

Use this command to accept and try BGP connections to external peers on indirectly connected networks. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Use the no parameter with this command to return to the default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop
neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255>
no neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop
no neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-255>	Maximum hop count

Default

By default, maximum hop count is 255

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.34 remote-as 20
(config-router)#neighbor 10.10.10.34 ebgp-multihop 5
```

neighbor enforce-multihop

Use this command to enforce BGP neighbors to perform multihop.

Use the no parameter with this command to turn off this feature.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop
no neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the maximum hop count is 255

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#neighbor 10.10.0.34 enforce-multihop
```

neighbor fall-over bfd

Use this command to create BFD session with BGP neighbor.

Use the no parameter with this command to delete BFD session with BGP neighbor.

Note: To have multihop BFD session with BGP neighbor, use 'multihop' option.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) fall-over bfd (multihop|)
no neighbor (A.B.C.D|X:X::X:X|WORD) fall-over bfd (multihop|)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, BFD session is not created with BGP neighbor.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
OcNOS(config)#router bgp 100
OcNOS(config-router)#neighbor 1.1.1.1 remote-as 100
OcNOS(config-router)#neighbor 2.2.2.2 remote-as 200
OcNOS(config-router)#neighbor 1.1.1.1 fall-over bfd multihop
OcNOS(config-router)#neighbor 2.2.2.2 fall-over bfd
OcNOS(config-router)#
```

neighbor filter-list

Use this command to set up a BGP filter. This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Name of an autonomous system path access list
in	Filter incoming advertised routes
out	Filter outgoing advertised route

Default

By default, filter list is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#neighbor 10.10.0.34 filter-list out in
```

neighbor limit

Use this command to specify the maximum number of peers that can be configured in the BGP dynamic peer-group.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor WORD limit <1-200>
no neighbor WORD (limit <1-200>|)
```

Parameters

WORD	Name of a BGP peer group created with the neighbor WORD peer-group command.
<1-200>	The maximum number of peers that can be configured in a BGP dynamic peer-group.

Default

By default, neighbor word limit is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor group1 limit 120
```

neighbor local-as

Use this command to specify an AS (autonomous system) number to use with BGP neighbor.

Use the no parameter with this command to disable this command.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>
no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-4294967295>	Neighbor's AS number when extended capabilities are configured

Note: The AS number 23456 is a reserved 2-byte AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default

By default, local as is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.34 local-as 12345
```

neighbor maximum-prefix

Use this command to set the number of prefixes that can be received from a neighbor.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295>
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> stop-update
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> warning-only
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100>
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100> warning-only
no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix
no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295>
no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> stop-update
no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> warning-only
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-4294967295>	Maximum number of prefixes accepted from this peer
stop-update	Stop installing routes when the maximum number of prefixes is exceeded.
warning-only	Only give a warning message when the maximum number of prefixes is exceeded. When this parameter is not specified and extra prefixes are received, the router ends the peering. A terminated peer remains down until the clear ip bgp A.B.C.D command is given.
<1-100>	Threshold value percent <1-100>

Default

By default, neighbor maximum prefix is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 maximum-prefix 1244 warning-only
```

neighbor next-hop-self

Use this command to make the router the next hop for a BGP-speaking neighbor or peer group. This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. Peers are reset and the new nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Use the no parameter with this command to disable this feature.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self
no neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, next hop self is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 remote-as 100
(config-router)#neighbor 10.10.0.72 next-hop-self
```

neighbor optional-as

Use this command to specify an AS (autonomous system) number to use with BGP dynamic peer-group.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor WORD optional-as <1-4294967295>
no neighbor WORD optional-as <1-4294967295>
```

Parameters

WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-4294967295>	The range from which the optional AS number must be configured.

Default

By default, neighbor optional as is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor group1 optional-as 400
```

neighbor override-capability

Use this command to ignore received capabilities and use locally configured values.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) override-capability
no neighbor (A.B.C.D|X:X::X:X|WORD) override-capability
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, override-capability is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 override-capability
```

neighbor passive

Use this command to make a BGP neighbor passive.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) passive
no neighbor (A.B.C.D|X:X::X:X|WORD) passive
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor passive is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 passive
```

neighbor authentication-key

Use this command to enable message digest5 (MD5) authentication on a TCP connection between two BGP peers. Configuring MD5 authentication between two BGP peers, means that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be established.

Use the no parameter with this command to delete the MD5 authentication.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key 0 <WORD>
no neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key 0 <WORD>
<WORD> plain text password

neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key <WORD>
no neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key <WORD>
<WORD> encrypted password
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of the BGP peer group
WORD	Password (Maximum length is 80 characters)

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 authentication-key 0 myPass

(config-router)#no neighbor 10.10.0.73 authentication-key 0 myPass
```

neighbor peer-group

Use this command to add a neighbor to an existing peer group. Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as distribute and filter lists. The peer group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer group, use the `neighbor WORD peer-group` command, and then use this command to add neighbors to the group.

Use the no parameter with this command to remove a neighbor from a named peer group.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X) peer-group WORD
no neighbor (A.B.C.D|X:X::X:X) peer-group WORD
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Peer group name

Default

Not applicable

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group
```

neighbor port

Use this command to set the BGP port number of a neighbor.

Use the no parameter with this command to remove a port number from a BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) port
no neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<0-65535>	Port number

Default

By default, neighbor port is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 port 643
```

neighbor prefix-list

Use this command to specify a prefix list for filtering BGP advertisements.

Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top. The neighbor distribute-list command is an alternative to this command and only one of them can be used to filter the same neighbor in any direction.

Use the no parameter with this command to remove an entry.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Name of an access list
in	Apply access list to incoming advertisements
out	Apply access list to outgoing advertisements

Default

By default, neighbor prefix list is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip prefix-list list1 deny 30.0.0.0/24
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 prefix-list list1 in
```

neighbor remote-as

Use this command to establish a BGP peering relationship with a customer edge router.

The specified neighbor only exchanges unicast address prefixes, unless the neighbor is also activated using the neighbor activate command, which allows the exchange of other routing information.

Use the no parameter with this command to delete this peering.

Note: BGP IPv6 VRF neighbor creation or activation is allowed in IPv6 VRF address-family and not allowed in IPv4 VRF address-family.

Note: BGP IPv4 VRF neighbor creation or activation is allowed in IPv4 VRF address-family and not allowed in IPv6 VRF address-family.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) remote-as <1-4294967295>
no neighbor (A.B.C.D|X:X::X:X|WORD) remote-as <1-4294967295>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-4294967295>	Neighbor's autonomous system number (ASN) when extended capabilities are configured. If the specified ASN matches the ASN number specified in the router BGP global configuration, the neighbor is identified as internal. If the ASN does no match, the neighbor is identified as external to the local AS.

Default

By default, neighbor remote is disabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 remote-as 345
(config-router)#neighbor 11.11.0.74 remote-as 23456
```

Note: The last command in the example above should be used when the local speaker is OBGP and the neighbor is NBGP with a 4-octet ASN.

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 remote-as 65000
```

```
(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 remote-as 65000
```

neighbor remove-private-AS

Use this command to remove the private autonomous system number (ASN) from outbound updates. Private ASNs are not advertised to the Internet. This command is used with external BGP peers only. The router removes the ASNs only if the update includes private ASNs. If the update includes both private and public ASNs, the system treats it as an error.

Use the no parameter with this command to revert to default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS
no neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor remove private AS is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.63 remove-private-AS
```

neighbor route-map

Use this command to apply a route map to incoming or outgoing routes. This command filters updates and modifies attributes. A route map is applied to inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

Use the no parameter with this command to a route map.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Name of the route map
in	Apply access list to incoming advertisements
out	Apply access list to outgoing advertisements

Default

Not applicable

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the configuration of the route map named rmap2 and then the use of this map name in the neighbor route-map command.

```
#configure terminal
(config)#route-map rmap2 permit 6
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 route-map rmap2 in
```

neighbor route-reflector-client

Use this command to make the router a BGP route reflector and set a specified neighbor as its client.

Using route reflectors reduces the number of iBGP peers within an AS. An AS can have more than one route reflector. A route reflector treats other route reflectors as other iBGP speakers.

Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client
no neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

Not applicable

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration, Router1 is the route reflector for clients 3.3.3.3 and 2.2.2.2; it also has a non-client peer 6.6.6.6.

```
#configure terminal
(config)#router bgp 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 3.3.3.3 route-reflector-client
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 2.2.2.2 route-reflector-client
(config-router)#neighbor 6.6.6.6 remote-as 200
```

neighbor route-server-client

Use this command to make a neighbor a route server client.

Use the no parameter with this command to remove the configuration of a neighbor as route server client.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client
no neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

Not applicable

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 route-server-client

#configure terminal
(config)#router bgp 10
(config-router)#no neighbor 10.10.0.72 route-server-client
```

neighbor send-community

Use this command to send that a community attribute to a BGP neighbor.

The community attribute groups destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes, the router reannounces them to the neighbor.

By default, both `standard` and `extended` community attributes are sent to a neighbor. To explicitly send only the `standard` or `extended` community attribute, run the bgp config-type command with the `standard` parameter before running this command.

Use the no parameter with this command to not announce community attributes to the neighbor. Use the `extended` and no parameters to remove extended communities. Specifying no other parameter with no removes standard communities only.

See also neighbor send-community in Chapter 4, *BGP Virtual Private Network Commands*.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) send-community
neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send Standard and Extended Community attributes
`extended`	Send Extended Community attributes
`standard`	Send Standard Community attributes

Default

Both `standard` and `extended` community attributes are sent to a neighbor.

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp config-type standard
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 send-community extended
```

neighbor send-label explicit-null

Use this command to exchange explicit –null label for the specific AF routes advertised between the neighbors. The AFI, SAFI combination of [1, 4] is the associated capability parameter (labelled-unicast) and is enabled by this command. This command is viable only on the ipv4 unicast and ipv4 vrf address families. This command has to be configured on both the neighbors for the capability to be negotiated.

Use the no parameter with this command to disable exchange of labels and remove the associated capability parameter.

Command Syntax

```
neighbor (WORD|x.x.x.x) send-label explicit-null
no neighbor (WORD|x.x.x.x) send-label explicit-null
```

Parameters

x.x.x.x	Address of the BGP neighbor in IPv4 format
WORD	Specify the neighbor router.

Default

By default, only the IPV4 unicast capability is enabled. Only configuration of this command on both neighbors will enable the Labelled Unicast capability.

Command mode

Address family and router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
# configure terminal
(config)# router bgp 100
(config-router)#neighbor 192.168.0.1 send-label explicit-null

# configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF-1
    (config-router-af)#neighbor 192.168.0.3 send-label explicit-null
```

neighbor shutdown

Use this command to terminate active sessions for a specified neighbor and clear all related routing information.

If a peer group is specified, a large number of peering sessions might be terminated. The `show ip bgp summary` command displays a summary of BGP neighbors and their connections.

Use the no parameter with this command to re-enable a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) shutdown
no neighbor (A.B.C.D|X:X::X:X|WORD) shutdown
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor shutdown is enabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 shutdown

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 shutdown
```

neighbor soft-reconfiguration inbound

Use this command to store updates for inbound soft reconfiguration.

Soft-reconfiguration can be used instead of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are re-processed according to the inbound policy. The BGP neighbor connection is not affected.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound
no neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the neighbor soft reconfiguration inbound is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 soft-reconfiguration inbound
```

neighbor strict-capability-match

Use this command to close the BGP connection if a capability value does not match the remote peer.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match
no neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, strict capability match is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 strict-capability-match
```

neighbor timers

Use this command to set the timers for a specific BGP neighbor.

Use the no parameter with this command to clear the timers for a BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) timers <0-65535> <0-65535>
neighbor (A.B.C.D|X:X::X:X|WORD) timers connect <1-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) timers
no neighbor (A.B.C.D|X:X::X:X|WORD) timers connect
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<0-65535>	Keepalive interval. Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router.
<0-65535>	Holdtime interval which is the time the router waits to receive a keepalive message. If the router does not receive a message in this period, the router declares the neighbor dead. The holdtime value should be at least 3 times the keepalive time.
connect	BGP connect timer
<1-65535>	Connect timer

Defaults

By default, keepalive timer value is 30 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 timers 60 230
(config-router)#neighbor 10.10.10.10 timers connect 10

(config-router)#no neighbor 10.10.10.10 timers
```

neighbor transparent-as

Use this command to not to append the AS path number even when the peer is an eBGP peer.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) transparent-as
```

Parameters

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, transparent as is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.7.1 transparent-as
```

neighbor transparent-nexthop

Use this command to keep the nexthop value of the route even when the peer is an eBGP peer.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) transparent-nexthop
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 transparent-nexthop
```

neighbor unsuppress-map

Use this command to selectively leak more-specific routes to a particular neighbor.

When the aggregate-address command is used with the `summary-only` option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the `neighbor unsuppress-map` command to selectively leak more-specific routes to a particular neighbor.

Use the no parameter with this command to restore the setting to the default level.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of the route map used to select routes to unsuppress

Default

By default, neighbor unsuppress map is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.73 unsuppress-map mymap

#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.70 unsuppress-map mymap
```

neighbor update-source

Use this command to allow internal BGP sessions to use any operating interface for TCP connections.

A loopback interface is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Use the no parameter with this command to restore the interface assignment to the closest interface.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) update-source WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) update-source
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Interface name

Default

By default, neighbor update source is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 update-source myif
```

neighbor version

Use this command to accept only a particular BGP version.

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2. Using this command disables the router's version-negotiation capability and forces the router to use only a specified version with the neighbor.

Use the no parameter with this command to use the default version level of a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) version 4
no neighbor (A.B.C.D|X:X::X:X|WORD) version
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
4	BGP version number

Default

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 version 4

(config)#router bgp 12
(config-router)#no neighbor 10.10.10.10 version
```

neighbor weight

Use this command to specify a weight value, per address-family, for all routes learned from a neighbor.

The route with the highest weight gets preference when the same prefix is learned from more than one peer. Unlike the local-preference attribute, the weight attribute is relevant only to the local router. The weights assigned using the `set weight` command override the weights assigned using this command.

Use this command in router mode to specify a weight value for all address families. Use this command in address family mode to specify a weight value per IPv4/IPv6/VPNv4/6PE address family,

When the weight is set for a peer group, all members of the peer group get the same weight. This command can also be used to assign a different weight to an individual peer-group member. When an individually-configured weight of a peer-group member is removed, its weight is reset to its peer group's weight.

Use the `no` parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) weight
no neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Weight value

Default

By default, neighbor weight value is 0

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 weight 60

(config-router)#no neighbor 10.10.10.10 weight 60
```

neighbor WORD peer-group

Use this command to create a peer group.

Use the no parameter with this command to remove a peer group.

Command Syntax

```
neighbor WORD peer-group
no neighbor WORD peer-group
```

Parameters

WORD	Name of BGP peer group

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to create a peer group named group1.

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group
```

network

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the `backdoor` parameter to specify a backdoor route to a BGP border router that will provide better information about the network. For data to be advertised by BGP, its routing table must include a route to the specified network. This command specifies the networks to be advertised. The network command works if the network being advertised is known to the router.

The `backdoor` parameter enables a route to be the preferred route even if it has a greater distance. A network that is specified as a backdoor network is dynamically assigned an administrative distance of 200 ensuring that IGP learned routes are preferred. If a backdoor network is not sourced by the local router, the network is learned from the external routers. If the route is learned from eBGP for a backdoor network, the distance is set to 20 or 200.

Use the `no` form of this command to remove a network route entry.

Command Syntax

```
network A.B.C.D (backdoor|)
network A.B.C.D/M (backdoor|)
network A.B.C.D mask A.B.C.D (backdoor|)
network A.B.C.D mask A.B.C.D route-map WORD (backdoor|)
network A.B.C.D route-map WORD (backdoor|)
network A.B.C.D/M route-map WORD (backdoor|)
no network A.B.C.D (backdoor|)
no network A.B.C.D/M (backdoor|)
no network A.B.C.D mask A.B.C.D (backdoor|)
no network A.B.C.D mask A.B.C.D route-map WORD (backdoor|)
no network A.B.C.D route-map WORD (backdoor|)
no network A.B.C.D/M route-map WORD (backdoor|)
```

Parameters

`A.B.C.D`	IP prefix <network>, for example, 35.0.0.0
`A.B.C.D/M`	IP prefix <network>/<length>, for example., 35.0.0.0/8
`backdoor`	BGP backdoor route
`routemap`	Route map used to modify the attributes
`WORD`	Name of the route map
`mask`	Network mask, for example, 255.255.0.0
`A.B.C.D`	Network mask, e.g., 255.255.0.0

Default

Not applicable

Command Mode

Router mode and Address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 is internally derived, that is, 2.0.0.0/8.

```
(config)#router bgp 1
(config-router)#network 2.0.0.0
```

network synchronization

Use this command to enable IGP synchronization for BGP static network routes.

Use this no parameter with this command to disable synchronization of BGP static routes.

Command Syntax

```
network synchronization
no network synchronization
```

Parameters

None

Default

By default, network synchronization is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables IGP synchronization of BGP static network routes in the router configuration mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#network synchronization
```

The following example enables IGP synchronization of BGP static network routes in the IPv6 unicast address-family mode.

```
#configure terminal
(config)#router bgp 11
(config)#address-family ipv6 unicast
(config-af)#network synchronization
```

redistribute

Use this command to inject routes from one routing process into another. Redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering is applied to make sure that only routes to be advertised reach the internet, not everything. This command allows redistribution by injecting prefixes from one routing protocol into another routing protocol.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute [connected|isis|kernel|ospf|rip|static]
redistribute [connected|isis|kernel|ospf|rip|static] route-map WORD
no redistribute [connected|isis|kernel|ospf|rip|static]
no redistribute [connected|isis|kernel|ospf|rip|static] route-map
no redistribute [connected|isis|kernel|ospf|rip|static] route-map WORD
```

Parameters

`connected`	Redistribute connected routes
`isis`	Redistribute connected ISO IS-IS routes
`kernel`	Redistribute connected kernel routes
`ospf`	Redistribute OSPFv2 routes
`rip`	Redistribute RIP routes
`static`	Redistribute static routes
`route-map`	Route map reference
`WORD`	Route map entries

Default

By default, redistribute is disabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the configuration of the route-map name `rmap1` and then the use of this map name in the `redistribute route-map` command.

```
#configure terminal
(config)#route-map rmap1 permit 1
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
```



```
(config-router)#redistribute ospf route-map rmap1

(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#redistribute static

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#redistribute static
```

router bgp

Use this command to start a BGP process.

Use the no form of this command to disable an existing routing process.

Command Syntax

```
router bgp <1-4294967295>
no router bgp <1-4294967295>
```

Parameters

`<1-4294967295>`

Associate the routing process with this autonomous system number

Default

Not applicable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#
```

snmp restart bgp

Use this command to restart SNMP in Border Gateway Protocol (BGP)

Command Syntax

```
snmp restart bgp
```

Parameters

None

Default

Not applicable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart bgp
```

synchronization

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems.

The `no synchronization` command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

Command Syntax

```
synchronization
no synchronization
```

Parameters

None

Default

Not applicable

Command Mode

Router mode and Address Family modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables IGP synchronization of iBGP routes in Router mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#synchronization
```

The following example enables IGP synchronization of iBGP routes in the IPv6-Unicast address family.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv6 unicast
(config-af)#synchronization
```

timers bgp

Use this command to globally set or reset the keepalive and holdtime values for all the neighbors.

Use the no parameter with this command to reset timers to default value.

Command Syntax

```
timers bgp <0-65535> <0-65535>
no timers bgp
no timers bgp <0-65535> <0-65535>
```

Parameters

<0-65535>	Frequency with which keepalive messages are sent to the neighbors
<0-65535>	Interval after which a neighbor is considered dead if keepalive messages are not received

Default

By default, keepalive timer value is 30 seconds

By default, holdtime value is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#timers bgp 40 120
```

CHAPTER 2 BGP Graceful Restart Commands

This chapter describes the BGP graceful restart commands.

bgp graceful-restart

Use this command to enable BGP graceful-restart capabilities. The restart-time parameter is used for setting the maximum time that a graceful-restart neighbor waits to come back up after a restart. This value is applied to all neighbors unless you explicitly override it by configuring the corresponding value on the neighbor. The stalepath-time parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stalepaths, unless reinstated by the neighbor after a re-establishment, will be deleted at the expiration of this timer.

Use the no parameter with this command to restore the router to its default state.

Command Syntax

```
bgp graceful-restart
bgp graceful-restart graceful-reset
bgp graceful-restart restart-time <1-3600>
bgp graceful-restart stalepath-time <1-3600>
no bgp graceful-restart
no bgp graceful-restart graceful-reset
no bgp graceful-restart restart-time
no bgp graceful-restart stalepath-time
```

Parameters

`graceful-reset`	The BGP daemon is not restarted, so that any changes in network configurations that cause BGP reset do not affect packet forwarding.
`restart-time`	Maximum time needed for neighbors to restart. Default is 90 seconds.
`<1-3600>`	Delay value in seconds.
`stalepath-time`	Maximum time to retain stale paths from restarting neighbors. Default is 360 seconds.
`<1-3600>`	Delay value in seconds.

Default

By default, the maximum time for neighbors to restart is 90 seconds.

By default, the maximum time to retain stale paths from restarting neighbors is 360 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#bgp graceful-restart

#configure terminal
(config)#router bgp 10
```



```
(config-router)#no bgp graceful-restart
```

bgp g-shut

Use this command to gracefully shut down all BGP IPv4 sessions under this router. The BGP graceful shutdown feature reduces packet loss during maintenance activity.

Use the no parameter with this command to bring up all the sessions under this router after completion of maintenance activity using the `bgp g-shut` command.

Command Syntax

```
bgp g-shut
no bgp g-shut
```

Parameters

None

Default

By default, bgp g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut

#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut
```

bgp g-shut-capable

Use this command to enable the graceful shutdown capability at the router level and make available the graceful-shutdown related commands at the router and BGP neighbor levels.

Use the no parameter with this command to disable the graceful shutdown capability on a router.

Note: The graceful shutdown capability cannot be disabled on a router that is in a graceful shutdown state until it comes out this state--after the graceful shutdown has been initiated and the impacted BGP sessions are up again.

Command Syntax

```
bgp g-shut-capable
no bgp g-shut-capable
```

Parameters

None

Default

By default, the graceful shutdown capability is disabled at the router level

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut-capable

#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut-capable
```

bgp g-shut-local-preference

Use this command to sets the local preference of the router to use during graceful shutdown. The local preference value indicates the preferred path when there are multiple paths to the same destination in a single routing database. The path with a higher preference value is the preferred one. The preferred path is sent to all routers and access servers in the local autonomous system.

Use the no parameter with this command to revert to the default setting.

Command Syntax

```
bgp g-shut-local-preference <0-4294967295>
no bgp g-shut-local-preference
```

Parameters

`<0-4294967295>` Local preference value

Default

By default, the local preference value is set to 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut-local-preference 22
```

bgp update-delay

Use this command to set the update delay for a graceful-restart capable router. The update-delay value is the maximum time a graceful-restart capable router, which is restarting, will defer route-selection and advertisements to all its graceful-restart capable neighbors. This maximum time starts from the instance the first neighbor attains established state after restart. The restarting router prematurely terminates this timer when end-of-RIB markers are received from all its graceful-restart capable neighbors.

Use the no form of this command to set to the update delay to its default value.

Command Syntax

```
bgp update-delay <1-3600>
no bgp update-delay
no bgp update-delay <1-3600>
```

Parameters

<1-3600>	Delay interval in seconds

Default

By default, update-delay value is 120 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#bgp update-delay 345
```

neighbor capability graceful-restart

Use this command to advertise the graceful restart capability to its neighbor. This configuration indicates that the BGP speaker has the ability to preserve its forwarding state for the address family when BGP restarts.

You must first specify a neighbor's `remote-as` identification number assigned by the neighbor router.

Note: The graceful restart capability is advertised only when the graceful restart capability has been enabled using the bgp graceful-restart command.

Use the `no` parameter with this command to not advertise the graceful restart capability to its neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart
no neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the graceful-restart is disabled

Command Mode

Router mode

Address family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.50 capability graceful-restart
```

neighbor g-shut

Use this command to start a graceful shutdown for the BGP session of the specified BGP neighbor. The BGP session for this neighbor is shut down after the graceful shutdown timer expires.

If there is no alternate path available for traffic to flow prior the actual shutdown of the BGP session, this path is made available for 60 seconds or for configured time after which the path is no longer available and traffic is dropped.

Use the `no` parameter with this command to bring up the session again for the specified BGP neighbor whose BGP session had been shut down using the `neighbor g-shut` command.

Note: The graceful shutdown capability is not supported on iBGP sessions.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) g-shut
no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut
```

Parameters

`A.B.C.D`	Neighbor IPv4 address
`X:X::X:X|`	Neighbor IPv6 address
`WORD`	Neighbor tag

Default

By default, neighbor g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut

#configure terminal
(config)#router bgp 100
(config-router)#no neighbor 1.1.1.2 g-shut
```

neighbor g-shut-timer

Use this command to configure the value of the graceful shutdown timer. After the timer expires, the BGP session initiated for graceful shutdown is shut down.

Use the no parameter with this command to revert to the default setting.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535>
```

Parameters

A.B.C.D	Neighbor IPv4 address
X:X::X:X	Neighbor IPv6 address
WORD	Neighbor tag
<10-65535>	Graceful shutdown timer in seconds

Default

By default, the timer value is set to 60 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut-timer 120
```

neighbor restart-time

Use this command to set a different restart-time than the global restart-time configured using the bgp graceful-restart command.

Use the no parameter with this command to restore the router to its default state.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600>
no neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-3600>	The maximum time that a graceful-restart neighbor waits to come back up after a restart. Make sure that this value does not exceed the stalepath-time specified in router mode.

Default

By default, restart time is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 restart-time 45
```

restart bgp graceful

Use this command to enable a BGP-speaker router for graceful restart. This command stops the whole BGP process and makes OcNOS retain the BGP routes and mark them as stale. Receiving BGP speakers, retain and mark as stale all BGP routes received from the restarting speaker for all address families received in the Graceful Restart Capability exchange.

Command Syntax

```
restart bgp graceful
```

Parameters

None

Default

By default, bgp graceful is disabled

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart bgp graceful
```

CHAPTER 3 BGP4+ Commands

This chapter describes the BGP4+ configuration commands.

- address-family ipv6 (see address-family in Chapter 1, *BGP Commands*)
- aggregate-address X:X::X:X/M
- bgp g-shut (see bgp log-neighbor-changes in n Chapter 1, *BGP Commands*)
- clear bgp * ipv6
- clear bgp ipv6 (A.B.C.D|X:X::X:X)
- clear bgp ipv6 <1-4294967295>
- clear bgp ipv6 external
- clear bgp ipv6 peer-group
- clear bgp ipv6 unicast flap-statistics
- clear bgp ipv6 unicast flap-statistics
- clear ipv6 bgp * vrf
- clear ipv6 bgp X:X::X:X vrf
- clear ip bpg ipv6 unicast table-map
- neighbor activate (see neighbor activate in Chapter 1, *BGP Commands*)
- neighbor attribute-unchanged (see neighbor attribute-unchanged in Chapter 1, *BGP Commands*)
- neighbor capability dynamic (see neighbor capability dynamic in Chapter 1, *BGP Commands*)
- neighbor capability route-refresh (see neighbor collide-established in Chapter 1, *BGP Commands*)
- neighbor default-originate (see neighbor default-originate in Chapter 1, *BGP Commands*)
- neighbor distribute-list (see neighbor distribute-list in Chapter 1, *BGP Commands*)
- neighbor filter-list (see neighbor filter-list in Chapter 1, *BGP Commands*)
- neighbor maximum-prefix (see neighbor maximum-prefix in Chapter 1, *BGP Commands*)
- neighbor next-hop-self (see neighbor next-hop-self in Chapter 1, *BGP Commands*)
- neighbor peer-group (see neighbor peer-group in Chapter 1, *BGP Commands*)
- neighbor prefix-list (see neighbor prefix-list in Chapter 1, *BGP Commands*)
- neighbor remove-private-AS (see neighbor remove-private-AS in Chapter 1, *BGP Commands*)
- neighbor route-map (see neighbor route-map in Chapter 1, *BGP Commands*)
- neighbor route-reflector-client (see neighbor route-reflector-client in Chapter 1, *BGP Commands*)
- neighbor send-community (see neighbor send-community in Chapter 1, *BGP Commands*)
- neighbor soft-reconfiguration inbound (see neighbor soft-reconfiguration inbound in Chapter 1, *BGP Commands*)
- neighbor unsuppress-map (see neighbor unsuppress-map in Chapter 1, *BGP Commands*)
- network X:X::X:X
- redistribute (see redistribute in Chapter 1, *BGP Commands*)

aggregate-address X:X::X:X/M

Use this command to configure BGP aggregate entries.

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. This command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the `summary-only` parameter advertises the prefix only, suppressing more-specific routes to neighbors.

The `as-set` parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use the `as-set` parameter to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. The `as-set` parameter is useful when aggregation of information results in an incomplete path information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
aggregate-address X:X::X:X/M
aggregate-address X:X::X:X/M as-set
aggregate-address X:X::X:X/M as-set summary-only
aggregate-address X:X::X:X/M summary-only
aggregate-address X:X::X:X/M summary-only as-set
no aggregate-address X:X::X:X/M
no aggregate-address X:X::X:X/M as-set
no aggregate-address X:X::X:X/M as-set summary-only
no aggregate-address X:X::X:X/M summary-only
no aggregate-address X:X::X:X/M summary-only as-set
```

Parameters

`X:X::X:X/M`	Aggregate IPv6 prefix
`as-set`	Generate AS set path information
`summary-only`	Filter more specific routes from updates

Command Mode

Address Family mode

Default

By default, aggregate address is disabled

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 2.2.2.2 remote-as 100
(config-router)#neighbor 3.3.3.3 remote-as 200
```

```
(config-router)#address-family ipv6
(config-router-af)#aggregate-address 3ffe::/32 as-set summary-only
```

clear bgp * ipv6

Use this command to reset the BGP IPv6 connection for all peers.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp ipv6 *
clear bgp ipv6 * in
clear bgp ipv6 * in prefix-filter
clear bgp ipv6 * out
clear bgp ipv6 * soft
clear bgp ipv6 * soft in
clear bgp ipv6 * soft out
clear ip bgp * ipv6 unicast in
clear ip bgp * ipv6 unicast out
clear ip bgp * ipv6 unicast soft
clear ip bgp * ipv6 unicast soft in
clear ip bgp * ipv6 unicast soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`unicast`	Unicast prefixes
`in`	Clear incoming advertised routes.
`out`	Soft reconfig outbound update
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Clear outgoing advertised routes

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp * ipv6 unicast soft out
```

clear bgp ipv6 (A.B.C.D|X:X::X:X)

Use this command to reset the BGP neighbor addresses (IPv4 or IPv6) for IPv6 peers.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp ipv6 (A.B.C.D|X:X::X:X)
clear bgp ipv6 (A.B.C.D|X:X::X:X) in
clear bgp ipv6 (A.B.C.D|X:X::X:X) in prefix-filter
clear bgp ipv6 (A.B.C.D|X:X::X:X) out
clear bgp ipv6 (A.B.C.D|X:X::X:X) soft
clear bgp ipv6 (A.B.C.D|X:X::X:X) soft in
clear bgp ipv6 (A.B.C.D|X:X::X:X) soft out
```

Parameters

`in`	Clear incoming advertised routes
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp ipv6 10.5.2.7
```

clear bgp ipv6 <1-4294967295>

Use this command to reset the BGP connection with a specified AS (Autonomous System) number for IPv6 peers.

Command Syntax

```
clear bgp ipv6 <1-4294967295>
clear bgp ipv6 <1-4294967295> in
clear bgp ipv6 <1-4294967295> in prefix-filter
clear bgp ipv6 <1-4294967295> out
clear bgp ipv6 <1-4294967295> soft
clear bgp ipv6 <1-4294967295> soft in
clear bgp ipv6 <1-4294967295> soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp ipv6 12345
```

clear bgp ipv6 external

Use this command to reset the BGP connection for all external IPv6 peers or for a specified external IPv6 peer.

Command Syntax

```
clear bgp ipv6 external
clear bgp ipv6 external in prefix-filter
clear bgp ipv6 external soft
clear bgp ipv6 external soft in
clear bgp ipv6 external soft out
clear bgp ipv6 external WORD in
clear bgp ipv6 external WORD out
```

Parameters

`in`	Clear incoming advertised routes
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update
`WORD`	Name of external IPv6 peer
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp ipv6 external soft in
```

clear bgp ipv6 peer-group

Use this command to reset the BGP connection for all members of a peer group.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear bgp ipv6 peer-group WORD
clear bgp ipv6 peer-group WORD in
clear bgp ipv6 peer-group WORD in prefix-filter
clear bgp ipv6 peer-group WORD out
clear bgp ipv6 peer-group WORD soft
clear bgp ipv6 peer-group WORD soft in
clear bgp ipv6 peer-group WORD soft out
```

Parameters

`in`	Clear incoming advertised routes
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update
`WORD`	BGP peer-group name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp peer-group P1
```

clear bgp ipv6 unicast flap-statistics

Use this command to reset IPv6 BGP route flap statistics.

Command Syntax

```
clear bgp ipv6 unicast flap-statistics
clear bgp ipv6 unicast flap-statistics X:X::X:X
clear bgp ipv6 unicast flap-statistics X:X::X:X/M
clear ip bgp ipv6 unicast flap-statistics
clear ip bgp ipv6 unicast flap-statistics X:X::X:X
clear ip bgp ipv6 unicast flap-statistics X:X::X:X/M
```

Parameters

`X:X::X:X`	IP prefix (network) for example, 35.0.0.0
`X:X::X:X/M`	IP prefix (network and length) for example, 35.0.0.0/8

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp ipv6 unicast flap-statistics 1:2::3:4/7
```

clear ipv6 bgp * vrf

Use this command to reset an IPv6 BGP connection for all virtual routing forwarding addresses.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ipv6 bgp * vrf WORD
clear ipv6 bgp * vrf WORD in
clear ipv6 bgp * vrf WORD out
clear ipv6 bgp * vrf WORD soft
clear ipv6 bgp * vrf WORD soft in
clear ipv6 bgp * vrf WORD soft out
```

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update
`WORD`	BGP peer-group name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 bgp * vrf BGPpeer7
```

clear ipv6 bgp X:X::X:X vrf

Use this command to reset the specified VPNv6 Routing/Forwarding (VRF) instance for BGP connections. If the neighbor address is specified with this command, it clears the specified connection. If no address is specified, this command clears all the BGP routes.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ipv6 bgp (X:X::X:X) vrf WORD
clear ipv6 bgp X:X::X:X vrf WORD in
clear ipv6 bgp X:X::X:X vrf WORD out
clear ipv6 bgp X:X::X:X vrf WORD soft in
clear ipv6 bgp X:X::X:X vrf WORD soft out
```

Parameters

`vrf`	Specify a VPN routing/forwarding instance for IPv6
`WORD`	VPN routing/forwarding instance name
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 bgp vrf 10:10::0:12 vrf vrfname
```

clear ip bpg ipv6 unicast table-map

Use this command to apply the modified table map or route map rules to the BGP routes in the existing IP routing table.

Command Syntax

```
clear ip bpg ipv6 unicast table-map (vrf (VRFNAME|all|default))
```

Parameters

`vrf`	Select a VPN Routing/Forwarding Instance.
`VRFNAME`	Specify a VPN Routing/Forwarding instance name.
`all`	Select all VRFs.
`default`	Select default VRFs.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp ipv6 unicast table-map vrf all
```

network X:X::X:X

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the `backdoor` parameter to specify a backdoor route to a BGP border router that will provide better information about the network. For data to be advertised by BGP, its routing table must include a route to the specified network. This command specifies the networks to be advertised. The network command works if the network being advertised is known to the router.

The `backdoor` parameter enables a route to be the preferred route even if it has a greater distance. A network that is specified as a backdoor network is dynamically assigned an administrative distance of 200 ensuring that IGP learned routes are preferred. If a backdoor network is not sourced by the local router, the network is learned from the external routers. If the route is learned from eBGP for a backdoor network, the distance is set to 20 or 200.

Use the `no` parameter with this command to remove an entry.

Command Syntax

```
network X:X::X:X/M
network X:X::X:X/M backdoor
network X:X::X:X/M route-map WORD (backdoor|)
no network X:X::X:X/M
no network X:X::X:X/M backdoor
no network X:X::X:X/M route-map WORD (backdoor|)
```

Parameters

`X:X::X:X`	IPv6 prefix <network>, for example, 3ffe::
`backdoor`	Specify a BGP backdoor route
`WORD`	Name of the route map

Default

No default value is specified

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 10
(config-router)#network 172.26.0.0/16
```

If Router1 receives updates from 172.10.0.0 via two routing protocols RIP (distance 120) and eBGP (distance 20), router1 chooses the shorter route. Use the `backdoor` parameter to allow Router1 to learn about 172.10.0.0 via RIP.

```
(config)#router rip
(config)#network 172.10.0.0
(config)#router bgp 200
```



```
(config)#neighbor 3.3.3.3 remote-as 500
(config)#network 172.10.0.0 backdoor
(config-router)#network 172.16.1.0/24 route-map myRM
```

CHAPTER 4 BGP Virtual Private Network Commands

This chapter describes the BGP Virtual Private Network (VPN) configuration commands.

- address-family (see address-family in Chapter 1, *BGP Commands*)
- bgp inbound-route-filter
- clear bgp * l2vpn vpls
- clear ip bgp * vpnv4
- clear bgp <1-4294967295> l2vpn vpls
- clear ip bgp <1-4294967295> vpnv4
- clear bgp A.B.C.D l2vpn vpls
- clear ip bgp A.B.C.D vpnv4
- debug bgp mpls
- exit-address-family (see exit-address-family in Chapter 1, *BGP Commands*)
- ip vrf
- neighbor activate (see neighbor activate in Chapter 1, *BGP Commands*)
- neighbor allow-ebgp-vpn
- neighbor allowas-in (see neighbor allowas-in in Chapter 1, *BGP Commands*)
- neighbor as-origination-interval (see neighbor as-origination-interval in Chapter 1, *BGP Commands*)
- neighbor as-override
- neighbor description (see neighbor description in Chapter 1, *BGP Commands*)
- neighbor remote-as (see neighbor remote-as in Chapter 1, *BGP Commands*)
- neighbor send-community (see neighbor send-community in Chapter 1, *BGP Commands*)
- neighbor shutdown (see neighbor shutdown in Chapter 1, *BGP Commands*)
- neighbor soo
- redistribute (see redistribute in Chapter 1, *BGP Commands*)
- rd (route distinguisher)
- route-target

bgp inbound-route-filter

Use this command to enable the MPLS (Multiprotocol Label Switching) VPN/BGP inbound route filter. This command is used to control the installation of routing information into the BGP table.

When a router runs MPLS VPN/BGP PE, it exchanges routing information with a routing distinguisher. By default, OcNOS does not install routing information that does not match the configured routing distinguisher value. When the local box has two VRFs where each routing distinguisher value is 10:100 and 20:200, routing information with routing distinguisher 10:200 is not installed into BGP table.

When `no bgp inbound-route-filter` is configured, all of routing information is installed into the BGP table.

Command Syntax

```
bgp inbound-route-filter
no bgp inbound-route-filter
```

Parameter

None

Default

By default, the router performs the routing distinguisher value check is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp inbound-route-filter
```

clear bgp * l2vpn vpls

Use this command to reset the session with all neighbors for VPLS address family

Command Syntax

```
clear bgp * l2vpn vpls
```

Parameters

None

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp * l2vpn vpls
```

clear ip bgp * vpnv4

Use this command to reset a VPNv4 BGP connection for all peers. This command clears the BGP connection and dynamically resets the outbound routing table. This frees up additional memory required for storing updates to generate new updates.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp * vpnv4 unicast in
clear ip bgp * vpnv4 unicast out
clear ip bgp * vpnv4 unicast soft
clear ip bgp * vpnv4 unicast soft in
clear ip bgp * vpnv4 unicast soft out
```

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp *
#clear ip bgp * vpnv4 unicast out
```

clear bgp <1-4294967295> l2vpn vpls

Use this command to reset the session for the neighbors with a specific ASN number for L2VPN VPLS.

Command Syntax

```
Clear bgp <1-4294967295> l2vpn vpls
```

Parameters

`<1-4294967295>` Autonomous System number of the BGP neighbor.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 100 l2vpn vpls
```

clear ip bgp <1-4294967295> vpnv4

Use this command to reset a BGP connection for all VPN peers in a specified Autonomous System.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp <1-4294967295> vpnv4 unicast in
clear ip bgp <1-4294967295> vpnv4 unicast out
clear ip bgp <1-4294967295> vpnv4 unicast soft
clear ip bgp <1-4294967295> vpnv4 unicast soft in
clear ip bgp <1-4294967295> vpnv4 unicast soft out
```

Parameters

`<1-4294967295>`	Clear peers with this AS number
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 500 vpnv4 unicast soft out
```

clear bgp A.B.C.D l2vpn vpls

Use this command to reset the session for neighbor with address A.B.C.D.

Command Syntax

```
clear bgp A.B.C.D l2vpn vpls
```

Parameters

A.B.C.D	BGP neighbor address.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 192.168.0.3 l2vpn vpls
```

clear ip bgp A.B.C.D vpnv4

Use this command to reset an VPNv4 BGP connection for a specific IPv4 address.

Note: The `soft in` or `in` and `soft out` or `out` in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp A.B.C.D vpnv4 unicast in
clear ip bgp A.B.C.D vpnv4 unicast out
clear ip bgp A.B.C.D vpnv4 unicast soft
clear ip bgp A.B.C.D vpnv4 unicast soft in
clear ip bgp A.B.C.D vpnv4 unicast soft out
```

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 10.10.0.12 vpnv4 unicast soft
#clear ip bgp 10.10.0.10 vpnv4 unicast out
```

debug bgp mpls

Use this command to enable the display of MPLS related information.

Use the `no` parameter with this command to disable this function.

Note: This command is available only when `vrf` option is enabled.

Command Syntax

```
debug bgp mpls
no debug bgp mpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
debug bgp mpls
```

ip vrf

Use this command to assign a VPN Routing Forwarding (VRF) instance.

Use the no option with this command to remove the VRF from the instance.

Command Syntax

```
ip vrf WORD
no ip vrf WORD
```

Parameter

WORD	Name of the VRF instance

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Command Example

```
(config)#ip vrf myVRF
(config-vrf)#
```

neighbor allow-ebgp-vpn

Use this command to allow an eBGP neighbor to be a VPN peer. By default, BGP VPN functionality is allowed only for iBGP peers.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn
no neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn
```

Parameters

A.B.C.D	Address of the BGP neighbor in IPv4 format
X:X::X:X	Address of the BGP neighbor in IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, BGP VPN functionality is allowed only for iBGP peers

Command Mode

Address Family-vpnv4 mode and Address Family-vpnv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 200
(config-router)#neighbor 66.66.66.66 remote-as 100
(config-router)#neighbor 66.66.66.66 update-source lo
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 66.66.66.66 allow-ebgp-vpn
(config-router-af)#neighbor 66.66.66.66 activate
(config-router-af)#exit-address-family
```

neighbor as-override

Use this command to configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider. BGP normally ignores routes from the same autonomous system. However, this command is used so that the Customer Edge (CE) routers router accepts and installs routes from the same autonomous system.

Typically, this command is used when CE routers have the same ASN in some or all sites. As per BGP requirement, a BGP speaker rejects a route that has the same ASN as itself in the AS_PATH attribute. Thus the CE routers having the same ASN do not accept routes from each other. Giving this command on the PE router removes the CE neighbor's ASN from the AS_PATH attribute allowing CE routers with the same ASN to accept routes from each other.

Use the no parameter with this command to remove VPN IPv4 prefixes from a specified router.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) as-override
no neighbor (A.B.C.D|X:X::X:X|WORD) as-override
```

Parameters

A.B.C.D	Address of the BGP neighbor in IPv4 format
X:X::X:X	Address of the BGP neighbor in IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor as override is disabled

Command Mode

Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 as-override

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 as-override
```

neighbor send-community

Use this command to send the extended-community attribute to a customer edge router. In VPN, the route-distinguisher and route-target are encoded in BGP extended-community.

See also neighbor send-community in Chapter 1, *BGP Commands*.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) send-community
neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send standard and extended community attributes
`extended`	Send extended community attributes
`standard`	Send standard community attributes

Default

By default, no extended-community attribute is sent to a customer router is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.10.1 remote-as 200
(config-router-af)#neighbor 10.10.0.1 send-community extended
```

neighbor soo

Use this command to enable the site-of-origin (SOO) feature. If the customer AS is multi-homed to the ISP, this command ensures that the PE does not advertise the routes back to the same AS.

Use the no parameter with this command to disable this feature.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) soo AS:nn_or_IP:nn
no neighbor (A.B.C.D|X:X::X:X|WORD) soo
```

Parameters

A.B.C.D	Address of the BGP neighbor in IPv4 format
X:X::X:X	Address of the BGP neighbor in IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
ASN:nn_or_IP-address:nn	An AS number and an arbitrary number (for example, 100:1), or a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

By default, the site-of-origin (SOO) feature is disabled.

Command Mode

Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 1.1.1.1 remote-as 200
(config-router-af)#neighbor 10.10.0.1 soo 100:1
```

rd (route distinguisher)

Use this command to assign a route distinguisher (RD) for the VRF. The route distinguisher value must be a unique value on the router.

This command creates routing and forwarding tables and specifies the default RD for a VPN. The RD is added to the customer's IPv4 prefixes, changing them into globally unique VPN-IPv4 prefixes.

Command Syntax

```
rd ASN:nn_or_IP-address:nn
```

Parameters

`ASN:nn_or_IP-address:nn`

AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#rd 100:1
```

route-target

Use this command to add a list of import and export route-target extended communities to the VRF.

This command creates lists of import and export route-target extended communities for the VRF. It specifies a target VPN extended community. Execute the command once for each community. All routes with the specific route-target extended community are imported into all VRFs with the same extended community as an import route-target.

Use the no parameter with this command to delete a route target.

Command Syntax

```
route-target (import|export|both) ASN:nn_or_IP-address:nn
no route-target (import|export|both) ASN:nn_or_IP-address:nn
```

Parameters

`import`	Import routing information
`export`	Export routing information
`both`	Import and export routing information
`ASN:nn_or_IP-address:nn`	AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#route-target both 100:10

(config)#ip vrf VRF_A
(config-vrf)#route-target import 100:20
```

CHAPTER 5 BGP Show Commands

This chapter describes the BGP show commands.

- show ip bgp peer-group vrf all
- show ip bgp rtfilter all
- show ip bgp scan
- show ip bgp vpnv4
- show ip bgp vpnv6 all neighbors
- show ip bgp vpnv6 rd neighbors
- show ip extcommunity-list
- show ip protocols
- show ip vrf

show bgp

Use this command to display the status of BGP routes.

Command Syntax

```
show bgp ipv4
show bgp (ipv6)
show bgp (ipv4|ipv6) (unicast|multicast)
show ip bgp
show ip bgp ipv4 (unicast|multicast)
show bgp (vrf (VRFNAME|all|default))
show ip bgp (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp ipv4
```

show bgp A.B.C.D

Use this command to display BGP route information for a network.

Command Syntax

```
show bgp (ipv4) (unicast|multicast) A.B.C.D
show ip bgp A.B.C.D
show ip bgp ipv4 (unicast|multicast) A.B.C.D
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D`	IP prefix (network), for example, 35.0.0.0

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip bgp 80.80.80.0

BGP routing table entry for 80.80.80.0/24
Paths: (1 available, no best path)
 Not advertised to any peer
 300
   15.15.15.1 (inaccessible) from 11.11.11.2 (15.15.15.2)
     Origin incomplete, metric 0, localpref 100, valid, internal
     rx path_id: 0      tx path_id: -1
     Last update: Wed May 11 15:22:36 2016
```

Table 5-108 explains the output fields.

Table 5-108: show ip bgp output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
LocalPref	Local preference value as set with the set local-preference route-map configuration command.
rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.

Table 5-108: show ip bgp output details

Field	Description
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

show bgp A.B.C.D/M

Use this command to display BGP route information for a network prefix.

Command Syntax

```
show bgp ipv4 (unicast|multicast) A.B.C.D/M
show ip bgp A.B.C.D/M
show ip bgp ipv4 (unicast|multicast) A.B.C.D/M
show ip bgp A.B.C.D/M (vrf (VRFNAME|all|default))
show ip bgp A.B.C.D/M longer-prefixes
show ip bgp ipv4 (unicast|multicast) A.B.C.D/M longer-prefixes
show ip bgp A.B.C.D/M longer-prefixes (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`longer-prefixes`	Display route and more specific routes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp ipv4 unicast 35.0.0.1/8
```

show bgp client

Use this command to display BGP client information.

Command Syntax

```
show bgp client
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
R1#sh bgp client
BGP client ID: 11
 PIM, socket 10
  Service: AS number service, Route Service
  Messsage received 1, sent 1
  Connection time: Tue May 14 03:11:01 2019
  Last message read: Service Request
  Last message write: Service Reply
R1#
```

show bgp community

Use this command to display BGP routes that match a community.

Command Syntax

```
show bgp ip (unicast|multicast) community
show bgp ip (unicast|multicast) community (vrf (VRFNAME|all|default))
show bgp ip (unicast|multicast) community [AA:NN|local-AS|no-advertise|no-export]
  (exact-match|)
show ip bgp community
show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-
  match|)
show ip bgp community (vrf (VRFNAME|all|default))
show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-
  match|)
show ip bgp community-list WORD (exact-match|) (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) community
show ip bgp ipv4 (unicast|multicast) community (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`AA:NN`	Community number
`local-AS`	Do not send outside local AS (well-known community)
`no-advertise`	Do not advertise to any peer (well-known community)
`no-export`	Do not export to next AS (well-known community)
`internet`	Internet community (well-known community)
`exact-match`	Exact match of the communities

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp community local-as no-export
```

```
#show bgp community local-AS exact-match
#show ip bgp ipv4 multicast community 12:34 exact-match
```

show bgp community-list

Use this command to display BGP routes that match a community list.

Command Syntax

```
show bgp community-list WORD (exact-match|)
show bgp ip (unicast|multicast) community-list WORD (exact-match|)
show bgp ip (unicast|multicast) community-list WORD (exact-match|)
show bgp (ipv4|ipv6) (unicast|multicast) community-list WORD (exact-match|)
show bgp (ipv6) community-list WORD (exact-match|)
show ip bgp community-list WORD (exact-match|)
show ip bgp ipv4 (unicast|multicast) community-list WORD (exact-match|)
```

Parameters

`WORD`	Community list name
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Only routes that exactly match the community

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp community-list mylist exact-match
#show ip bgp ipv4 multicast community-list mylist exact-match
```

show bgp dampening dampened-paths

Use this command to display detailed information about paths suppressed due to dampening.

Command Syntax

```
show bgp dampening dampened-paths
show bgp (ipv4|ipv6) (unicast|multicast) dampening dampened-paths
show bgp (ipv6) dampening dampened-paths
show ip bgp dampening dampened-paths
show ip bgp dampening dampened-paths (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) dampening dampened-paths
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp dampening dampened-paths
BGP table version is 32, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                 Reuse   Path
 d   11.11.11.0/24    90.90.90.1            00:27:20 200 i
```

Table 5-108 shows the status codes displayed at the start of a route entry.

Table 5-109: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale **.**
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

Table 5-113 shows the codes at the end of each route entry that indicate where the route originated.

Table 5-110: origin details

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 5-114 explains the output fields.

Table 5-111: show bgp dampening dampened-paths output details

Field	Description
Network	Internet address of a network.
From	IP address of the advertising peer.
Reuse	The amount of time remaining until this route will be un-suppressed and can be used again.
Path	Autonomous system path to the destination network.

show bgp dampening flap-statistics

Use this command to display BGP dampening flap statistics.

Command Syntax

```
show bgp dampening flap-statistics
show bgp (ipv4|ipv6) (unicast|multicast) dampening flap-statistics
show bgp (ipv6) dampening flap-statistics
show ip bgp dampening flap-statistics
show ip bgp dampening flap-statistics (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) dampening flap-statistics
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This sample output shows that the internal route (`i`), has flapped 3 times and is now categorized as history (h).

```
#show ip bgp dampening flap-statistics
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From               Flaps  Duration  Reuse   Path
hi1.1.1.0/24     10.100.0.62       3  00:01:20       i
```

Table 5-108 shows the status codes displayed at the start of a route entry.

Table 5-112: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale **.**
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

Table 5-113 shows the codes at the end of each route entry that indicate where the route originated.

Table 5-113: origin details

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 5-114 explains the output fields.

Table 5-114: show bgp dampening flap-statistics output details

Field	Description
Network	Internet address of a network.
From	IP address of the advertising peer.
Flaps	Number of times this route has failed and returned (flapped).
Duration	Elapsed time since the first penalty points were assessed.
Reuse	The amount of time remaining until this route will be un-suppressed and can be used again.
Path	Autonomous system path to the destination network.

show bgp dampening parameters

Use this command to display the BGP dampening parameters.

Command Syntax

```
show bgp dampening parameters
show bgp (ipv4|ipv6) (unicast|multicast) dampening parameters
show bgp (ipv6) dampening parameters
show ip bgp dampening parameters
show ip bgp ipv4 (unicast|multicast) dampening parameters (vrf
  (VRFNAME|all|default))
show ip bgp dampening parameters (vrf (VRFNAME|all|default))
```

Parameters

ipv4	IPv4 routes
ipv6	IPv6 routes
unicast	Unicast prefixes
multicast	Multicast prefixes
VRFNAME	VPN routing/forwarding instance name
all	All VRFs
default	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip bgp dampening parameters
 dampening 5 750 2000 60 15
 Dampening Control Block(s):
  Reachability Half-Life time    : 5 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reachability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
#
```

Table 5-115 explains the output fields.

Table 5-115: show ip bgp dampening parameters output details

Field	Description
Dampening Control Block(s)	Flap damping reduces the number of update messages by marking routes as ineligible for selection as the active or preferable route.
Reachability Half-Life time	Number of minutes after which an arbitrary value is halved if a route stays stable.
Reuse penalty	Reuse threshold—Arbitrary value below which a suppressed route can be used again.
Suppress penalty	Cutoff (suppression) threshold—Arbitrary value above which a route can no longer be used or included in advertisements.
Max suppress time	Maximum hold-down time for a route, in minutes.
Un-reachability Half-Life time	Number of minutes after which an arbitrary value is not halved if a route stays stable.
Max penalty (ceil)	Maximum penalty corresponds to the time it would take max-suppress to decay and reach the reuse level (ceil).
Min penalty (floor)	Maximum penalty corresponds to the time it would take max-suppress to decay and reach the reuse level (floor).

show bgp filter-list

Use this command to display routes that match a regular expression filter list.

Command Syntax

```
show bgp filter-list WORD
show bgp (ipv4|ipv6) (unicast|multicast) filter-list WORD
show bgp (ipv6) filter-list WORD
show ip bgp filter-list WORD
show ip bgp ipv4 (unicast|multicast) filter-list WORD
show ip bgp filter-list WORD (exact-match)
show ip bgp filter-list WORD (exact-match) (vrf (VRFNAME|all|default))
show ip bgp filter-list WORD (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) filter-list WORD (exact-match)(vrf
  (VRFNAME|all|default))
```

Parameters

`WORD`	Regular-expression filter list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the filter list
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp filter-list mylist
```

show bgp inconsistent-as

Use this command to display routes with inconsistent AS paths.

Command Syntax

```
show bgp inconsistent-as
show bgp (ipv4|ipv6) (unicast|multicast) inconsistent-as
show bgp (ipv6) inconsistent-as
show ip bgp inconsistent-as
show ip bgp ipv4 inconsistent-as
show ip bgp ipv4 (unicast|multicast) inconsistent-as
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp inconsistent-as
```

show bgp ipv6

Use this command to display the BGP routing table.

Command Syntax

```
show bgp ipv6 (unicast|multicast|labeled|)
show bgp ipv6 (unicast|multicast|labeled|) X:X::X:X/M
```

Parameters

`multicast`	IPv6 multicast address prefixes
`unicast`	IPv6 unicast address prefixes
`labeled`	Labeled IPv6 routes
`X:X::X:X/M`	IPv6 prefix network/length, such as 3ffe:a::/64

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: iBGP and eBGP Routes

This example shows routes learned from both iBGP and eBGP.

```
#show bgp ipv6
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal S stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                                    Metric LocPrf Weight  Path
*> 2001:58::/32                                                 0  20 ?
     fe80::202:b3ff:fec8:9fdb
*> 2002:58::/32                                                 0  20 i
     fe80::202:b3ff:fec8:9fdb
*>i2003:58::/32                                      100        0  i
     fe80::208:a1ff:fe16:797d
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- BGP table version
- BGP router ID is `10.100.0.77`

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```

Table 5-108 shows the status codes displayed at the start of a route entry.

Table 5-116: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale **.**
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

Origin codes: i - IGP, e - EGP, ? - incomplete

Table 5-117 shows the codes at the end of each route entry that indicate where the route originated.

Table 5-117: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Route Entry Examples

```
*> 2002:58::/32     fe80::202:b3ff:fec8:9fdb                              0 20 i
```

- This route entry shows that this route is learned from eBGP.
- The origin code “i” means that the prefix is added by the network statement at originating AS.
- The path 20 indicates that the prefix advertisement originated from AS20.
- The administrative weight parameter applies only to routes within an individual router.
- Since this route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

```
*> 2001:58::/32      fe80::202:b3ff:fec8:9fdb                              0 20 ?
```

- This route entry shows that the prefix is learnt from eBGP.The origin code i indicates that the prefix is added by network statement at originating AS.The path attribute 20 indicates that the route advertisement originated from AS20.The administrative weight parameter applies only to routes within an individual router. Since this route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.The origin code “?” means the route was learned through redistribution.

```
*>i2003:58::/32      fe80::208:a1ff:fe16:797d                    100     0 i
```

- The status code “i” means that the route was learned through iBGP. The Local Preference attribute of the route, which is used only with the local AS, is set to 100 (the default value).

Example: IPv6 Prefix Routes

This example shows labeled routes for a given IPv6 prefix:

```
#show bgp ipv6 labeled 3ffe:a::/64
          BGP routing table entry for 3ffe:a::/64
          Paths: (1 available, best #1, table Default-IP-Routing-Table)
          Not advertised to any peer
          Local
          ::ffff:114:1414 from 20.20.20.1 (92.92.92.92)
          Origin incomplete metric 0, localpref 100, label    5420,
          valid, internal, best
          Last update: Mon May 26 17:48:18 2008
```

Table 5-118 explains the output fields.

Table 5-118: show bgp ipv6 output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
LocalPref	Local preference value as set with the set local-preference route-map configuration command.
rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

show bgp l2vpn vpls

Command Syntax

```
show bgp l2vpn vpls (rr|) (detail|)
```

Parameters

`rr`	Display the information of auto-discovered peers at Route reflector node.
`detail`	Display the detailed information of auto-discovered peers.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced in version OcNOS version 1.3.

Example

```
#show bgp l2vpn vpls
VPLS-ID   VE-ID    Discovered-Peers   Route-Target
10        3        1                   10:100


#show bgp l2vpn vpls  detail

VPLS ID: 10
VE-ID: 3
Discovered Peers: 1
Route-Target: 10:100
Local RD: 10:100
 Mesh Peers:
  Address:3.3.3.3, RD:10:100, VE-ID:4
  VC Details: VC-ID:34
  Remote (LB:52480,VBO:1,VBS:64)  Local (LB:52480,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:52483, Out Label:52482
  PW Status:Established
```

Table 5-119 explains the output fields.

Table 5-119: show bgp l2vpn vpls output details

Field	Description
VPLS-ID	L2VPN address family database information for the Virtual Private LAN Service (VPLS).
VE-ID	L2VPN address family database information for the Virtual Expansion.
Discovered Peers	Peer discovery is used to find peers that are available for data using LLDP.
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.

Table 5-119: show bgp l2vpn vpls output details

Field	Description
Local RD	The Local Route Descriptor – the first two numbers of the Route-Target.
Mesh Peers	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.
Address	Mesh session information for the peer specified with the ip-address argument.
RD	Mesh peer's Route-Descriptor.
VC Details	The virtual circuit session information with the ip-address for the Provider Edge (PE) routers.
Remote	LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. VBS (VE Block Size) – the size of the label block.
Local	LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. VBS (VE Block Size) – the size of the label block.
LB sent on known VEID	Whether the Label Base came on a known Virtual Expansion Identifier – yes or no.
In Label	The ingress (incoming interface) label for this segment.
Out Label	Label received from downstream neighbor for route.
PW Status	The status of the VPLS Pseudo-Wire. Values can be: Idle, Active, Open, or Established.

```
#show bgp l2vpn vpls rr
RD        RR-Clients     Non-Clients          Route-Target
10:100     2                  0                 10:100
10:100     2                  0                 10:100


#show bgp l2vpn vpls rr detail

Route-Target: 10:100
  Peer:1.1.1.1
    RR Client  : Yes
    VE-ID:3  LB:52480  VBO:1  VBS:64

Route-Target: 10:100
  Peer:3.3.3.3
    RR Client  : Yes
    VE-ID:4  LB:52480  VBO:1  VBS:64
```

Table 5-120 explains the output fields.

Table 5-120: show bgp l2vpn vpls rr output details

Field	Description
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.
Peer	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.
RR Client	Device is a client of the Route Reflector – yes or no.
VE-ID	L2VPN address family database information for the Virtual Expansion.
LB	LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain.
VBO	VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router.
VBS	VBS (VE Block Size) – the size of the label block.

show bgp neighbors

Use this command to display information about BGP neighbor connections.

Command Syntax

```
show bgp neighbors
show bgp ipv6 neighbors
show ip bgp ipv4 (unicast|multicast) neighbors
show ip bgp neighbors
show ip bgp neighbors (A.B.C.D|X:X::X:X)(advertise-routes|)
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X)
show ip bgp neighbors (A.B.C.D|X:X::X:X) (hold-time|keepalive-interval|connection-
  retrytime)
show ip bgp neighbors (A.B.C.D|X:X::X:X) (sent-msgs|rcvd-
  msgs|notification|update|open|keepalive
```

Parameters

`ipv4`	IPv4 neighbors
`ipv6`	IPv6 neighbors
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`advertised-routes`	Routes advertised to a BGP neighbor
`hold-time`	Hold time
`keepalive-interval`	Keepalive interval
`connection-retrytime`	Connection retry time
`sent-msgs`	Sent packets
`rcvd-msgs`	Received packets
`notification`	Notification messages
`update`	Update messages
`open`	Open messages
`keepalive`	Keepalive messages

Command Mode

Privileged Exec and Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group myPeer for session parameters
  BGP version 4, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  myPeer peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network
Last Reset: 00:32:48, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

BGP Neighbor Fields

Table 5-121 explains the output fields.

Table 5-121: show bgp neighbor output details

Field	Description
BGP neighbor	BGP session information for the neighbor with the ip-address argument.
remote AS	Remote Autonomous system used to exchange exterior routing information between neighboring ASs.
local AS	Local Autonomous system used to exchange internal routing information within AS.

Table 5-121: show bgp neighbor output details

Field	Description
internal link external link	Internal link is used to forward route advertisements received from an external BGP router through the internal network (in the same AS). External link is used for exchanging routing information between Autonomous Systems (AS) and routing traffic across the Internet (eBGP neighbor).
member of peer-group	Peer group information for the peer group specified with the peer-group argument.
BGP version	Negotiated BGP version for this session.
remote router ID	IP address of the neighbor. BGP uses the highest loopback address as the Router ID. If no loopback interface is configured, BGP uses the highest configured IP address on a system.
BGP state	Session state as explained in Table 5-126. The exchange of routing information begins between peers only after the neighbor session is in an Established state.
up for	Time that the underlying TCP connection has been up.
last read	Time since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages. The maximum time that can elapse between successive messages from this neighbor is 180 seconds. If no message is received for 180 seconds, this neighbor will be declared dead.
last write	Time since BGP last sent a message to this neighbor.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor. The time interval between successive keepalive messages is 60 seconds. Typically, the hold time value is set to three times the keepalive interval.
neighbor capabilities	BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers.
received	Total number of received messages. notifications: Number of notification (error) messages received. in queue: Number of messages in the input queue
sent	Total number of sent messages. notifications: Number of notification (error) messages sent. in queue: Number of messages in the output queue
route refresh request	Number of route refresh request messages sent and received.
minimum time between advertisement runs.	The minimum time gap, in seconds, between successive route updates sent to the neighbor. Generally, a jitter (of 25%) is applied to this time interval, which means that if the time between advertisements is configured as 30, successive advertisements can have a time gap of as low as 22.5 (after applying a 25% jitter to the 30 seconds, which is 7.5 seconds).
for address family	The peers have exchanged address family capability.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. “Dropped” means the number of time the connection has failed or gone down.

Table 5-121: show bgp neighbor output details

Field	Description
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

show bgp neighbors advertised-routes

Use this command to display the routes advertised to a BGP neighbor.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes (vrf
  (VRFNAME|all|default))
show ip bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) advertised-routes
```

Parameters

`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`ipv4`	IPv4 addresses
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp ipv4 multicast neighbors 1.2.3.4 advertised-routes
```

show bgp neighbors received prefix-filter

Use this command to display the prefix list filter.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X) received prefix-filter
show ip bgp neighbors (A.B.C.D|X:X::X:X) received prefix-filter
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received prefix-
  filter
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp neighbors 1.2.3.4 received prefix-filter
```

show bgp neighbors received-routes

Use this command to display the received routes from a neighbor.

To display all the received routes from a neighbor, perform a BGP soft reconfigure first.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X) received-routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X) received-routes
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp neighbors 10.10.10.2 received-routes
```

show bgp neighbors routes

Use this command to display all accepted routes learned from neighbors.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X) routes
show ip bgp neighbors (A.B.C.D|X:X::X:X) routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) routes
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following output displays detailed information about the neighbor.

```
#show bgp neighbors 10.10.10.2 routes
BGP neighbor is fe80::203:47ff:feb0:d72b, remote AS 10, local AS 10, internal
link
  BGP version 4, remote router ID 10.10.10.50
  BGP state = Established, up for 00:02:01
  Last read 00:00:01, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

Table 5-122 explains the output fields.

Table 5-122: show bgp neighbors routes output details

Field	Description
BGP neighbor	Neighbor identifier along with the local and remote Autonomous System numbers.
BGP version	The version of BGP being used by the neighbor device, along with the remote router ID number.
BGP state	The current state of the neighbor connection and length of time within the current state. Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours**:** Minutes**:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: 1. Route refresh 2. Address family IPv4 Unicast 3. Address family IPv6 Unicast
Route refresh	This helps to identify that and synchronize the peers without a hard reset.
For address family	Address Family Identifier (AFI) IPv4 Unicast.
Received messages	Information received from the neighbors.
notifications	Passes information to a router about sessions.
in que	Number of messages currently residing in the queue awaiting action.
Route refresh request	Information received and sent.
Minimum time between advertisement runs	Interval between exchange of messages.
For address family: IPv4 Unicast	The following three values are subordinate to the IPv4 Unicast Address Family.
Community attributes sent to this neighbor	Both the standard and the extended community information has been sent to the neighbor.
accepted prefixes	Configure a limit to the number of prefixes that can be accepted in a BGP peer session.
announced prefixes	A prefix announced in BGP consists of the IPV4 or IPV6 address block being announced.

show bgp nexthop-tracking

Use this command to display BGP nexthop-tracking status.

Command Syntax

```
show bgp nexthop-tracking
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp nexthop-tracking

Configured NHT: ENABLED
NHT Delay time-interval : 6
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0

BGP VRF: VRF_A VRF_ID 2
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0
```

Table 5-123 explains the output fields.

Table 5-123: show bgp nexthop-tracking output details

Field	Description
Configured NHT	Whether Next Hop Tracking (NHT) is enabled or disabled.
NHT Delay time-interval	A delay timer that indicates how long this device waits before checking its RIB for changes.

Table 5-123: show bgp nexthop-tracking output details

Field	Description
BGP VRF	Name and ID number of this BGP VRF.
BGP Instance	Autonomous System number and router ID.
NHT is Enabled	NHT Network enables the measurement and comparison of performance.
Recvd Msg count from RIB	Number of received change-messages from the RIB.
NHT delay-timer remaining seconds	Time remaining until the next decision cycle.
BGP nexthop(s)	Nexthop in the BGP to reach a certain destination.
Total number of IPV4 nexthops	Number of nexthops in the IPv4 Address Family.
Total number of IPV6 nexthops	Number of nexthops in the IPv6 Address Family.

show bgp nexthop-tree-details

Use this command to display BGP nexthop-tree details.

Command Syntax

```
show bgp nexthop-tree-details
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp nexthop-tree-details
BGP Instance: (Default), AS: 65534, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0

BGP Instance: (Default), AS: 0, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0
```

Table 5-124 explains the output fields.

Table 5-124: show bgp nexthop-tree-details output details

Field	Description
Bgp Instance	The Autonomous System number and router ID.
AFI_IP Nexthop count	Nexthop count for the IPv4 Address Family
AFI_IP6 Nexthop count	Nexthop count for the IPv6 Address Family

show bgp paths

Use this command to display BGP path information.

Command Syntax

```
show bgp paths
show bgp (ipv6) paths
show ip bgp paths
show ip bgp ipv4 (unicast|multicast) paths
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp paths

Address        Refcnt    Path
[0x1af8ee0:0]   (21)
[0x1b3ceb0:345] (14)     64602
[0x1c71d40:821] (12008)  64602 65500
[0x1d03fb0:822] (12008)  64602 65501
```

Table 5-125 explains the output fields.

Table 5-125: show bgp paths output details

Field	Description
Address	Hash and hash key separated by the colon character.
Refcnt	Number of routed using that path.
Path	Autonomous System Number (ASN) for the route.

show bgp prefix-list

Use this command to display routes matching the prefix-list.

Command Syntax

```
show bgp prefix-list WORD
show bgp (ipv4|ipv6) (unicast|multicast|) prefix-list WORD (vrf
  (VRFNAME|all|default|))
show ip bgp prefix-list WORD
show ip bgp prefix-list WORD (exact-match)
show ip bgp prefix-list WORD (exact-match) (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) prefix-list WORD
show ip bgp ipv4 (unicast|multicast) prefix-list WORD (exact-match)
```

Parameters

`WORD`	Name of the IP prefix list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the prefix list
`vrf`	VPN Routing/Forwarding instance
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp prefix-list mylist
```

show bgp quote-regexp

Use this command to display route matching an AS path quoted regular expression.

Command Syntax

```
show bgp quote-regexp WORD
show bgp (ipv4|ipv6) (unicast|multicast|) quote-regexp WORD
show ip bgp quote-regexp WORD
show ip bgp ipv4 (unicast|multicast) quote-regexp WORD
```

Parameters

`WORD`	A regular expression to match the AS paths. Use quotes to enclose the regular expression.
`ipv4`	IPv4 route information
`ipv6`	IPv6 route information
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp quote-regexp "myPath"
```

show bgp regexp

Use this command to display routes matching the AS path regular expression.

Command Syntax

```
show bgp regexp LINE
show bgp (ipv4|ipv6) (unicast|multicast) regexp LINE
show bgp (ipv6) regexp LINE
show ip bgp regexp LINE
show ip bgp regexp LINE (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) regexp LINE
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`LINE`	A regular expression to match the AS paths
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp regexp myPath
```

show bgp route-map

Use this command to display routes that match the specified route map.

Command Syntax

```
show bgp route-map WORD
show bgp (ipv4|ipv6) (unicast|multicast) route-map WORD
show bgp (ipv6) route-map WORD
show ip bgp route-map WORD
show ip bgp route-map WORD (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) route-map WORD
```

Parameters

`WORD`	Routes matching the route-map
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`vrf`	VPN routing/forwarding instance
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp route-map myRM
```

show bgp statistics

Use this command to display BGP statistics.

Command Syntax

```
show bgp statistics
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp statistics

============================================================
BGP VRF default statistics
============================================================
Neighbor aggregated statistics (sent/received)
Msgs          Bytes           Opens          Updates
16/17           394/0           1/2          0/0
Keepalives  Notifications  Route-refresh  Capabilities
15/15            0/0           0/0          0/0
BGP I/O Information
Active Open attempts            : 0
Passive Open attempts           : 0
BGP I/O Open loops              : 0
BGP I/O Open calls              : 0
BGP I/O Open recv calls         : 0
BGP I/O Send calls              : 0
BGP I/O Recv calls              : 0
BGP I/O Write calls             : 0
BGP I/O Write loops             : 0
BGP I/O Write loop yields       : 0
BGP I/O Read calls              : 0
BGP I/O Read loops              : 0
BGP I/O Read loop yields        : 0
BGP I/O process nlri yields     : 0
BGP I/O process withdraw yields : 0
BGP Read time exceeded          : 0
BGP Update send pending         : 0
BGP Update buffer not available : 0
BGP Update walk suspended       : 0
BGP Yielded in updates          : 0
BGP Yielded in packing          : 0
BGP No sendbuf for peer         : 0
BGP No withdraw buf for peer    : 0
BGP Yields in update peer loop  : 0
```

```
No updates pending or no buffers: 0
No data to write                : 0
Msg queue recv errors           : 0
Sockets create/accept/close     : 2/1/2
Sockets create retries/failures : 1/0
Socket fd-close session         : 0
MemPool - Advertise             : | Total (0/0) blk_size:64
MemPool - AdjOut                : | Total (0/0) blk_size:12
MemPool - Advertise Attr        : | Total (0/0) blk_size:24
MemPool - BGP Info              : | Total (0/0) blk_size:216
MemPool - BGP Attr              : | Total (0/0) blk_size:224
MemPool - BGP Node IPv4         : | Total (0/0) blk_size:128
MemPool - BGP Node IPv6         : | Total (0/0) blk_size:136
MemPool - BGP Node EVPN         : | Total (0/0) blk_size:160
MemPool - BGP Node Max KeyLen   : | Total (0/0) blk_size:176
MemPool - BGP RIB msg4          : | Total (0/0) blk_size:4440
MemPool - BGP RIB msg6          : | Total (0/0) blk_size:424
MemPool - BGP MPLS REQ          : | Total (0/0) blk_size:32
#
```

show bgp summary

Use this command to display a summary of BGP neighbor status.

Command Syntax

```
show bgp summary
show bgp (ipv4|ipv6) (unicast|multicast|) summary
show ip bgp summary
show ip bgp summary (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) summary
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp summary

BGP router identifier 6.6.6.6, local AS number 64601

BGP table version is 1

1 BGP AS-PATH entries

0 BGP community entries

Neighbor V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd

*12.1.1.24 64902    7          7       1      0      0   00:02:54       0

* Dynamically created based on a listen range command

BGP dynamic peer-group: group1
```

```
listen range:  12.1.0.0/16
Total number of dynamically created neighbors/limit: 1/(200)
Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
Total number of neighbors 1
Total number of Established sessions 1

BGP dynamic peer-group: group2
listen range:  12.2.0.0/16
Total number of dynamically created neighbors/limit: 0/(200)
Total number of dynamically created neighbors: 0
Total number of activated dynamic peer-groups for IPv4 Unicast address-family: 1
```

Header

```
BGP router identifier 10.10.15.50, local AS number 65000
1 BGP AS-PATH entries
0 BGP community entries
```

- The BGP router identifier is 10.10.15.50 and the local router AS number is 65000.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- There is one BGP AS-PATH entry and no community entries.

Neighbor Entry Fields

Table 5-126 explains the fields for each neighbor entry.

Table 5-126: neighbor entry fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.
MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.
OutQ	Messages waiting in the output queue to be sent.

Table 5-126: neighbor entry fields (Continued)

Field	Description
Up/Down	Connection up time and down time.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keepalive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keepalive messages with its peer Invalid: The session state is invalid

Neighbor Entry Example

```
10.10.14.51   4   100  93       120     0      0    0     00:42:16        0
```

- The neighbor has the IP address 10.10.14.51 and AS number 100.
- The neighbor uses BGP version 4.
- 93 messages have been received.
- 120 messages have been sent.
- The BGP routing table version is 0.
- There are no received messages waiting in the input queue for further processing.
- There are no messages waiting in the output queue to be sent.
- The connection has been up for 0 hours, 42 minutes and 53 seconds.
- The local router has received no prefixes from this neighbor.

show bgp view

Use this command to display information for a BGP view.

Command Syntax

```
show bgp ipv6 view WORD
show ip bgp view WORD
show ip bgp view WORD A.B.C.D
show ip bgp view WORD A.B.C.D/M
show ip bgp view WORD ipv4 (unicast|multicast) summary
show ip bgp view WORD neighbors
show ip bgp view WORD neighbors (A.B.C.D|X:X::X:X)
show ip bgp view WORD summary
```

Parameters

ipv6	IPv6 addresses
WORD	BGP view name
A.B.C.D	Network in the BGP routing table
A.B.C.D/M	IP prefix <network>/<length>, e.g., 35.0.0.0/8, in the BGP routing table
ipv4	IPv4 addresses
multicast	Multicast prefixes
unicast	Unicast prefixes
summary	Summary of BGP neighbor status
neighbors	Detailed information on TCP and BGP neighbor connections
A.B.C.D	IPv4 neighbor
X:X::X:X	IPv6 neighbor

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp view I2
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i100.156.70.0/24  10.10.10.52                  0      0 i
*>i100.156.71.0/24  10.10.10.52                  0      0 i
*>i100.156.72.0/24  10.10.10.52                  0      0 i
```

```
*>i100.156.73.0/24  10.10.10.52                    0      0 i
*>i100.156.74.0/24  10.10.10.52                    0      0 i

Total number of prefixes 5
```

show bgp X:X::X:X

Use this command to display BGP network information in an IPv6 environment.

Command Syntax

```
show bgp X:X::X:X
show bgp (ipv6) X:X::X:X
show bgp (ipv6) (unicast|multicast) X:X::X:X
```

Parameters

`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`X:X::X:X`	IPv6 prefix (network), for example, 2003::

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp ipv6 3ffe::8
```

show bgp X:X::X:X/M longer prefixes

Use this command to display BGP network information along with mask information.

Command Syntax

```
show bgp X:X::X:X/M longer-prefixes
```

Parameters

`X:X::X:X/M`	IPv6 prefix (network/length), for example, 2003::/16

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp 3ffe::8/8 longer-prefixes
```

show debugging bgp

Use this command to display BGP debugging options.

Command Syntax

```
show debugging bgp
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the show debugging bgp command.

```
#show debugging bgp
BGP debugging status:
 BGP debugging is on
 BGP events debugging is on
 BGP updates debugging is on
 BGP fsm debugging is on
```

show ip bgp

Use this command to display BGP routes.

Command Syntax

```
show ip bgp
show ip bgp ipv4 (unicast|multicast)(vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows routes learned from both iBGP and eBGP peers.

```
#show ip bgp
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale,
      Origin codes: i - IGP, e - EGP,? - incomplete
       Network             Next Hop      Metric LocPrf   Weight   Path
   *> 172.16.1.0/24     10.10.10.78                          0       1 4 i
   *> 192.16.1.0        10.10.10.78       200                0       1 4 ?
   *                    10.100.0.62       100                0       3 4 ?
   *>i 192.17.1.0       10.100.0.62                 100      0       i

Total number of prefixes 2
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- The Router ID of the local router is `10.100.0.77`.

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```

Table 5-127 explains the status codes in the header.

Table 5-127: status codes

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and will not be advertised to the neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The route selected as the best path and installed in the kernel routing table.
i	internal	Whether the route is learned from an iBGP peer. If this symbol is not present, the route was learned from an eBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 5-128 explains the codes are at the end of each routing entry that show where the route originated.

Table 5-128: origin codes

Origin code	Description	Comments
i	IGP	The route originated from an Interior Gateway Protocol.
e	EGP	The route originated from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an Interior Gateway Protocol.

Route Entry Fields

Table 5-129 explains the fields shows for each route.

Table 5-129: route entry fields

Field	Description
Network	Network prefix installed in BGP. If multiple routes exist for the same prefix, only the first prefix is identified and others have blank spaces. The status codes are explained in Table 5-127.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.

Table 5-129: route entry fields (Continued)

Field	Description
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.
Path and origin	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 5-128

Route Entry Examples

```
*> 172.16.1.0/24     10.10.10.78                            0    1 4 i
```

- The absence of status code “i” means the route is external and was learned from an eBGP peer.
- The “>” means this route is selected to be installed in the kernel routing table. Its network address is 172.16.1.0/24.
- The IP address of the nexthop for this route is 10.10.10.78.
- This route was learned from a peer, so it has a default weight of 0.
- The path “1 4” means the prefix advertisement passed through AS1 and AS4.
- The origin code “i” means the prefix was added by a network statement at an originating AS.

```
*> 192.16.1.0        10.10.10.78            200            0    1 4 ?
*                    10.100.0.62            100            0    3 4 ?
```

- The same prefix was learned from two different ASs, AS1 and AS3.
- The route learned from AS1 is chosen as the best route because AS1 has a lower Router ID (10.10.10.78) than AS2 (10.100.0.62). Although the metric of the route learned from AS1 is higher (200) than the route learned from AS3 (100), this attribute is not used in the best path selection decision because the metrics are compared only if the first (neighboring) AS is the same in the two paths.
- The origin code “?” indicates that the routes were learned through redistribution.

```
*>i192.17.1.0        10.100.0.62                     100     0    i
```

- The route is learned through an iBGP peer as indicated by the status code “i”.
- The preference of the route, used only with the local AS, is 100 (the default value).

show ip bgp cidr-only

Use this command to display routes with non-natural network masks.

Command Syntax

```
show ip bgp cidr-only
show ip bgp ipv4 (unicast|multicast) cidr-only
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip bgp cidr-only` command.

```
#show ip bgp cidr-only
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24       10.10.10.10                              0 11 i
Total number of prefixes 2
```

show ip bgp community-info

Use this command to list all BGP community information.

Command Syntax

```
show ip bgp community-info
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp community-info

Address Refcnt Community
```

show ip bgp peer-group

Use this command to list the BGP peer group information.

Command Syntax

```
show ip bgp peer-group <name>
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp peer-group group1
BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group members:
  12.1.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```

show ip bgp peer-group vrf all

Use this command to list all BGP peer group VRF information.

Command Syntax

```
show ip bgp peer-group vrf all
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp peer-group vrf all
% VRF: VRF1

BGP dynamic peer-group is group2, EBGP, remote AS 64902
  BGP dynamic peer-group group2 listen range group members:
  12.2.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
% VRF: management
Peer-Group not found

% VRF: default

BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group members:
  12.1.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```

show ip bgp rtfilter all

Use this command to display route target filters sent and received.

Command Syntax

```
show ip bgp rtfilter all
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp rtfilter all
```

show ip bgp scan

Use this command to display BGP scan status.

Command Syntax

```
show ip bgp scan
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60 secs
scan remain-time: 3 secs
Current BGP nexthop cache:
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
```

show ip bgp vpnv4

Use this command to display information relating to VPNv4.

Command Syntax

```
show ip bgp vpnv4 all
show ip bgp vpnv4 all A.B.C.D
show ip bgp vpnv4 all neighbors
show ip bgp vpnv4 all neighbors A.B.C.D
show ip bgp vpnv4 all summary
show ip bgp vpnv4 all tags
show ip bgp vpnv4 rd WORD
show ip bgp vpnv4 rd WORD A.B.C.D
show ip bgp vpnv4 rd WORD label
show ip bgp vpnv4 rd WORD neighbors
show ip bgp vpnv4 rd WORD neighbors A.B.C.D
show ip bgp vpnv4 rd WORD summary
show ip bgp vpnv4 view WORD all
show ip bgp vpnv4 vrf NAME
show ip bgp vpnv4 vrf NAME A.B.C.D
show ip bgp vpnv4 vrf NAME label
show ip bgp vpnv4 vrf NAME summary
```

Parameters

`all`	Displays information about all VPNv4 NLRIs
`A.B.C.D`	Network
`neighbors`	TCP and BGP neighbor connections
`A.B.C.D`	Network
`summary`	Summary display
`tags`	BGP tags for prefixes
`rd`	Route distinguisher
`WORD`	BGP view name
`A.B.C.D`	Network
`label`	MPLS Labels for prefixes
`neighbors`	TCP and BGP neighbor connections
`A.B.C.D`	Network
`summary`	Summary display
`view`	VPNv4 NLRI-specific information
`WORD`	BGP view name

`vrf`	VRF VPNv4 NLRIs
`NAME`	VPN Routing/Forwarding instance name
`A.B.C.D`	Network
`label`	MPLS Labels for prefixes
`summary`	Summary display

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip bgp vpnv4 all` command displaying VPNv4 specific information

```
#show ip bgp vpnv4 all
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (VRF1)
* i 10.10.9.0/24     10.10.0.1                0   141      0  65000 ?
*>  10.10.9.0/24     10.10.14.50              0            0  65000 ?
*>  10.10.10.0/24    10.10.14.50                           0  65000 ?
* i 10.10.15.0/24    10.10.0.1                    141      0  65000 ?
*>  10.10.15.0/24    10.10.14.50              0            0  65000 ?

#show ip bgp vpnv4 all neighbors

BGP neighbor is 24.10.10.2, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 179.112.0.1
  BGP state = Established, up for 10:04:14
  Last read 10:04:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: received
    Address family IPv6 Unicast: received
  Received 1641 messages, 0 notifications, 0 in queue
  Sent 1280 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 676, neighbor version 676
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  60000 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 24.10.10.1, Local port: 179
Foreign host: 24.10.10.2, Foreign port: 32959
Nexthop: 24.10.10.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Table 5-130 explains the fields shows for each route.

Table 5-130: show ip bgp vpnv4 all neighbors output details

Field	Description
BGP neighbor	Router ID of the BGP neighbor.
remote AS	Autonomous system number of the neighbor.
local AS	Autonomous system number of the local system.
internal link	internal link: iBGP neighbor (in the same AS).
BGP version	The version of BGP being used by the neighbor device.
BGP state	The current state of the neighbor connection and length of time within the current state.Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours **:** Minutes **:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: 1. Route refresh 2. Address family IPv4 Unicast 3. Address family IPv6 Unicast
Received	Message count, notification count, number of messages waiting in the queue.
Sent	Message count, notification count, number of messages waiting in the queue.
Route refresh request	Route requests sent and received.
For address family	As stated – in this case IPv4 Unicast.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. “Dropped” means the number of time the connection has failed or gone down.
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.

Table 5-130: show ip bgp vpnv4 all neighbors output details (Continued)

Field	Description
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

show ip bgp vpnv6 all neighbors

Use this command to display VPNv6 NLRI information for all neighbors or for a given neighbor.

Command Syntax

```
show ip bgp vpnv6 all neighbors
show ip bgp vpnv6 all neighbors (A.B.C.D|X:X::X:X)
```

Parameters

A.B.C.D	IPv4 neighbor address
X:X::X:X	IPv6 neighbor address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ip bgp vpnv6 all neighbors
BGP neighbor is 10.32.0.3, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 10.32.0.2, remote router ID 10.32.0.3
  BGP state = Established, up for 00:37:31
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
  Received 25711 messages, 0 notifications, 0 in queue
  Sent 25673 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 837, neighbor version 837
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

```
 For address family: VPNv6 Unicast
  BGP table version 302, neighbor version 302
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.32.0.2, Local port: 179
Foreign host: 10.32.0.3, Foreign port: 38416
Nexthop: 10.32.0.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:37:34, due to Hold Timer Expired (Notification sent)
Notification Error Message: (Hold Timer Expired/No sub-error code)

BGP neighbor is 101.101.1.2, vrf 1, remote AS 101, local AS 1, external link
  BGP version 4, local router ID 101.101.1.1, remote router ID 0.0.0.0
  BGP state = Idle
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 512 messages, 0 notifications, 0 in queue
  Sent 450 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 27, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 1

BGP neighbor is 101.102.1.2, vrf 2, remote AS 102, local AS 1, external link
  BGP version 4, local router ID 101.102.1.1, remote router ID 0.0.0.0
  BGP state = Idle
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 511 messages, 0 notifications, 0 in queue
  Sent 449 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 26, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes
```

```
 Connections established 1; dropped 1

BGP neighbor is 101.103.1.2, vrf 3, remote AS 103, local AS 1, external link
  BGP version 4, local router ID 101.103.1.1, remote router ID 0.0.0.0
  BGP state = Idle
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 511 messages, 0 notifications, 0 in queue
  Sent 452 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 26, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 1

BGP neighbor is 101.104.1.2, vrf 4, remote AS 104, local AS 1, external link
  BGP version 4, local router ID 101.104.1.1, remote router ID 0.0.0.0
  BGP state = Connect
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 511 messages, 0 notifications, 0 in queue
  Sent 449 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 27, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 1
Next connect timer due in 108 seconds

BGP neighbor is 101.105.1.2, vrf 5, remote AS 105, local AS 1, external link
  BGP version 4, local router ID 101.105.1.1, remote router ID 0.0.0.0
  BGP state = Idle
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 511 messages, 0 notifications, 0 in queue
  Sent 454 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 26, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
```

```
  0 announced prefixes

 Connections established 1; dropped 1
```

show ip bgp vpnv6 rd neighbors

Use this command to display VPNv6 NLRI information for a given route distinguisher and optionally for a given neighbor.

Command Syntax

```
show ip bgp vpnv6 rd WORD neighbors
show ip bgp vpnv6 rd WORD neighbors (A.B.C.D|X:X::X:X)
```

Parameters

WORD	Route distinguisher
A.B.C.D	IPv4 neighbor address
X:X::X:X	IPv6 neighbor address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ip bgp vpnv6 rd 1:1 neighbors
BGP neighbor is 10.32.0.3, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 10.32.0.2, remote router ID 10.32.0.3
  BGP state = Established, up for 00:43:57
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
  Received 25726 messages, 0 notifications, 0 in queue
  Sent 25689 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 837, neighbor version 837
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv6 Unicast
  BGP table version 302, neighbor version 302
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
```

show ip extcommunity-list

Use this command to display BGP routes that match an extended community list.

Command Syntax

```
show ip extcommunity-list (WORD | )
show ip extcommunity-list (<1-199>|WORD)
show ip bgp extcommunity-list WORD (exact-match|)(vrf VRFNAME|)
```

Parameters

WORD	Name of extended community list
<1-199>	Number of extended community list
VRFNAME	VPN routing/forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip extcommunity-list 33
```

show ip protocols

Use this command to display information about the IP protocols such as IP routing process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols bgp
```

Parameters

bgp	BGP information

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip protocols bgp
Routing Protocol is "bgp 100"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain
   eth0                2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
 Distance: (default is 120)
```

Table 5-131 explains the fields shows for each route.

Table 5-131: show ip protocols output details

Field	Description
Routing Protocol is "bgp 100"	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.
Next due in 12 seconds	Precisely when the next update is due to be sent.
Timeout after 180 seconds	Specifies the value of the timeout parameter.
Redistributing	Lists the protocol that is being redistributed.

Table 5-131: show ip protocols output details

Field	Description
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the IP Infusion software is using to build its routing table.

show ip vrf

Use this command to display the routing information of the VRF, such as interface, route distinguisher, route-target, and so on.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	VRF name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip vrf VRF_A
VRF VRF_A; (table=1)
```

Appendix A Regular Expressions

Table A-132 shows the regular expression special characters used in BGP commands. You can use these characters in combination to build complex regular expressions.

Table A-132: Regular expression characters

Symbol	Character	Meaning
^	Caret	Matches the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Matches the end of the input string.
.	Period	Matches a single character (including white spaces).
*	Asterisk	Matches none or more sequences of a pattern.
+	Plus sign	Matches one or more sequences of a pattern.
?	Question mark	Matches none or one occurrence of a pattern.
_	Underscore	Matches spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[]	Brackets	A range of single-characters.
-	Hyphen	Separates the end points of a range.

VRF Lite Configuration Guide

Contents

This document contains these chapters and appendices:

CHAPTER 1 BGP Configuration

Overview

Border Gateway Protocol (BGP) makes core routing decisions on the Internet using a table of IP networks or “prefixes” which designate network reachability among autonomous systems (AS). BGP is a path vector protocol or a variant of a distance-vector routing protocol. BGP does not involve traditional Interior Gateway Protocol (IGP) metrics, but routing decisions are made based on path, network policies, and/or rule sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol.

Topology

Figure 1-64: BGP topology for VRF

Configuration

R1

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#rd 800:1`	Specify the route distinguisher in the VRF
`(config-vrf)#route-target import 800:1`	Specify the import route target
`(config-vrf)#route-target export 800:1`	Specify the export route target
`(config-vrf)#exit`	Exit VRF mode
`(config)#router bgp 200`	Enter the bgp configuration mode
`(config-router)#address-family ipv4 vrf  vrf1`	Enter address family mode for vrf1
`(config-router-af)#neighbor 2.2.2.2 remote-as 100`	Specify the BGP neighbor and remote-AS.
`(config-router-af)#exit`	Exit address family mode.
`(config-router)#ex`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address 2.2.2.1 to eth1

R2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Create vrf1

(config-vrf)#rd 800:1	Specify the route distinguisher in the VRF
(config-vrf)#route-target import 800:1	Specify the import route target
(config-vrf)#route-target export 800:1	Specify the export route target
(config-vrf)#exit	Exit vrf mode
(config)#router bgp 100	Enter router mode.
(config-router)#address-family ipv4 vrf vrf1	Enter address family mode for vrf1
(config-router-af)#neighbour 2.2.2.1 remote-as 200	Specify the BGP neighbor and remote-as.
(config-router-af)#exit	Exit address family mode.
(config-router)#ex	Exit router mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ip address 2.2.2.2/24	Configure the IP address 2.2.2.1 to eth1

Validation

Verify the routing table in R1:

```
#show ip bgp neighbors
BGP neighbor is 2.2.2.2, vrf vrf1, remote AS 2, local AS 1, external link
  BGP version 4, remote router ID 3.3.3.2
  BGP state = Established, up for 00:00:00
  Last read 00:00:00, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 48116
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Verify the routing table in R2:

```
#show ip bgp neighbors
```

```
BGP neighbor is 2.2.2.1, vrf vrf1, remote AS 1, local AS 2, external link
  BGP version 4, remote router ID 2.2.2.1
  BGP state = Established, up for 00:02:01
  Last read 00:02:01, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.2, Local port: 179
Foreign host: 2.2.2.1, Foreign port: 48116
Nexthop: 2.2.2.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
[II]
```

R1

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1

Gateway of last resort is not set
```

R2

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
```

```
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1

Gateway of last resort is not set
```

Verify BGP Adjacency

Use the following show commands to verify the BGP adjacency:

```
show ip bgp neighbor
```

CHAPTER 2 VRF Configuration

Overview

Virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. VRF may be implemented in a network device by distinct routing tables known as forwarding information bases – one per routing instance.

Topology

Figure 2-65: Device topology

Default VRF

`#con t`	Enter the router configuration mode
`(config)#interface eth1`	Switch to interface eth1
`(config-if)#ip address 3.3.3.2/24`	Configure the ip address **`3.3.3.2`** to eth1
`(config-if)#exit`	Exit interface mode.

Adding a Static Route

`#con t`	Enter the router configuration mode
`(config)#ip route  20.20.20.0/24 eth1`	Add static route with eth1 as exit interface

User-Defined VRF

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1. Use no ip vrf vrf-1 to delete the created vrf
`(config)#exit`	Exit configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate eth1 to vrf1. Use no ip vrf forwarding vrf1 for un-configuration

(config-if)#ip address 3.3.3.2/24	Configure the IP address 3.3.3.2 to eth1
(config-if)#exit	Exit interface mode.

Adding a Static Route

#con t	Enter the router configuration mode
(config)# ip route vrf vrf1 20.20.20.0/24 eth1	Add static route in vrf1 with eth1 as exit interface

Validation

```
#show ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     127.0.0.0/8 is directly connected, lo, 00:14:59
C     192.168.52.0/24 is directly connected, eth0, 00:14:55
IP Route Table for VRF "management"
IP Route Table for VRF "vrf1"
C     3.3.3.0/24 is directly connected, eth1, 00:00:44
S     20.20.20.0/24 [1/0] is directly connected, eth1, 00:00:08

Gateway of last resort is not set
```

To display the IP routing table associated with a VRF, use the show ip route vrf vrf-name command

```
#sh ip route vrf vrf-1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf-1"
C            3.3.3.0/24 is directly connected, eth1, 00:01:22
S            20.20.20.0/24 [1/0] is directly connected, eth1, 00:00:13

Gateway of last resort is not set
```

Use this show command to display the static routes configured

```
#sh ip route vrf  vrf-1 static
     IP Route Table for VRF "vrf-1"
     S            20.20.20.0/24 [1/0] is directly connected, eth1, 00:01:13

     Gateway of last resort is not set
```

CHAPTER 3 OSPF Configuration

Overview

Open Shortest Path First (OSPF) is an interior routing protocol operating within a single autonomous system (AS) that uses a link state routing algorithm. OSPF gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet layer which makes routing decisions based solely on the destination IP address in IP packets.

This chapter covers OSPF configuration in non-default VRF.

Topology

Figure 3-66: OSPF topology for VRF

Configuration IPv4 VRF

R1

`#con t`	Enter the router config mode.
`(config)#ip vrf vrf1`	Create vrf1
`((config-vrf)#exit`	Exit VRF mode
`(config)#router ospf 1 vrf1`	Associate the ospf process with vrf1.
`(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0.
`(config-router)#ex`	Exit the OSPF configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Associate eth1 to vrf1.
`(config-if)#ip address 2.2.2.1/24`	Assign the IP address 2.2.2.1 to eth1 in vrf1

R2

`#con t`	Enter the router config mode
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#exit`	Exit VRF mode
`(config)#router ospf 1 vrf1`	Associate the ospf process with vrf1
`(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0.

(config-router)#ex	Exit router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Associate eth1 to vrf1.
(config-if)#ip address 2.2.2.2/24	Assign the IP address 2.2.2.1 to eth1 in vrf1

Validation

R1

```
#show ip ospf neighbor
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State       Dead Time   Address    Interface Instance ID
2.2.2.2         1   Full/Backup   00:00:30   2.2.2.2     eth1       0

#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1
Gateway of last resort is not set
```

R2

```
#show ip ospf neighbor
OSPF process 1 VRF(vrf1):
Neighbor ID   Pri   State    Dead Time   Address         Interface Instance ID
2.2.2.1       1   Full/DR    00:00:35    2.2.2.1           eth1    0

#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1
Gateway of last resort is not set
```

CHAPTER 4 ISIS Configuration

Overview

Intermediate System to Intermediate System (IS-IS) is an interior routing protocol operating within a single administrative domain.It is a link-state routing protocol, operating by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination.

Topology

Figure 4-67: ISIS Topology for VRF

Configuration IPv4 VRF

R1

`#configure terminal`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#exit`	Exit VRF mode
`(config)#router isis 1 vrf1`	Associate the ISIS process to vrf1
`(config-router)#net 49.0001.0000.0000.0001.00`	Establish a network entity title for this instance, specifying the area address and the system ID.
`(config-router)#is-type level-1`	Configure instance 1 as level-1 routing
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address 2.2.2.1 to eth1
`(config-if)#ip router isis 1`	Enable ISIS routing on an instance for area 49
`(config-if)#isis circuit-type level-1`	Configure interface as level-1
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

R2

#con t	Enter configuration mode.
(config)#ip vrf vrf1	Create vrf1
(config-vrf)#exit	Exit VRF mode
(config)#router isis 1 vrf1	Associate the ISIS process to vrf1
(config-router)#net 49.0001.0000.0000.0002.00	Establish a network entity title for this instance, specifying the area address and the system ID.
(config-router)#is-type level-1	Configure instance 1 as level-1 routing
(config-router)#exit	Exit router mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ip address 2.2.2.2/24	Configure the IP address 2.2.2.1 to eth1
(config-if)#ip router isis 1	Enable ISIS routing on an instance for area 49
(config-if)#isis circuit-type level-1	Configure interface as level-1
(config-if)#exit	Exit interface mode
(config)#exit	Exit config mode

Validation

R1

```
#show clns neighbors
Tag 1:  VRF : vrf1
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.000d.52f0      Up     28        L1   IS-IS
```

R2

```
#show clns neighbors
Tag 1:  VRF : vrf1
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.000d.52f0      Up     28        L1   IS-IS
```

R1

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag 1:  VRF : vrf1
     Destination         Metric      Next-Hop            Interface      Tag
C    2.2.2.0/24         10         --                eth1          0            0
```

R2

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
```

```
Tag 1:  VRF : vrf1
     Destination          Metric      Next-Hop            Interface      Tag
C    2.2.2.0/24          10          --                 eth1           0            0
```

CHAPTER 5 ISIS IPv6 VRF Configuration

Overview

Intermediate System to Intermediate System (IS-IS) is an interior routing protocol operating within a single administrative domain.It is a link-state routing protocol, operating by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination.

Topology

Figure 5-68: ISISv6 Topology for VRF

R1

`#configure terminal`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#exit`	Exit VRF mode
`(config)#router isis 1 vrf1`	Associate the ISIS process to vrf1
`(config-router)#net 49.0001.0000.0000.0001.00`	Establish a network entity title for this instance, specifying the area address and the system ID.
`(config-router)#is-type level-1`	Configure instance 1 as level-1 routing
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ipv6 address 1000::1/64`	Configure ipv6 address on eth1
`(config-if)#ipv6 router isis 1`	Enable ISISv6 routing on an instance for area 49
`(config-if)#isis circuit-type level-1`	Configure interface as level-1
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

R2

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1

(config-vrf)#exit	Exit VRF mode
(config)#router isis 1 vrf1	Associate the ISIS process to vrf1
(config-router)#net 49.0001.0000.0000.0002.00	Establish a network entity title for this instance, specifying the area address and the system ID.
(config-router)#is-type level-1	Configure instance 1 as level-1 routing
(config-router)#exit	Exit router mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ipv6 address 1000::2/64	Configure ipv6 address on eth1
(config-if)#ipv6 router isis 1	Enable ISISv6 routing on an instance for area 49
(config-if)#isis circuit-type level-1	Configure interface as level-1
(config-if)#exit	Exit interface mode
(config)#exit	Exit config mode

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : vrf1
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     27        L1   IS-IS
R1#
R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag 1:  VRF : vrf1
C    1000::/64 [10]
      via ::, eth1

R1#

#
R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : vrf1
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     8         L1   IS-IS
R2#
R2#show ipv6 isis route
```

```
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag 1:  VRF : vrf1
C    1000::/64 [10]
      via ::, eth1

R2#
```

Open Shortest Path First Command Reference

Contents

This document contains these chapters and appendices:

CHAPTER 1 OSPFv2 Commands

This chapter provides an alphabetized reference for each of the OSPFv2 commands. It includes the following commands:

- show ip ospf database detail
- show ip ospf igp-shortcut-lsp
- show ip ospf igp-shortcut-route
- show ip ospf interface
- show ip ospf multi-area-adjacencies
- show ip ospf neighbor
- show ip ospf route
- show ip ospf valid
- show ip ospf virtual-links
- show ip protocols
- show ip route fast-reroute
- shutdown
- snmp restart ospf
- summary-address
- timers lsa arrival
- timers spf exp
- timers throttle lsa

area authentication

Use this command to enable authentication for an OSPF area. Specifying the area authentication sets the authentication to Type 1 authentication or simple text password authentication (details in RFC 2328). Setting up a Type 1 authentication configures a 64-bit field for that particular network. All packets sent on this network must have this configured value in their OSPF header. This allows only routers that have the same passwords to join the routing domain. Give all routers that are to communicate with each other through OSPF the same authentication password.

Use the ip ospf authentication-key command to specify a simple text password.

Use the ip ospf message-digest-key command to specify an MD5 password.

Use the no parameter to remove the authentication specification for an area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) authentication
area (A.B.C.D|<0-4294967295>) authentication message-digest
no area (A.B.C.D|<0-4294967295>) authentication
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as 4-octet unsigned integer value.
`message-digest`	Enables MD5 authentication in the specified area ID.

Default

Null authentication

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 authentication message-digest

(config)#router ospf 100
(config-router)#no area 1 authentication
```

area default-cost

Use this command to specify a cost for the default summary route sent into a stub or NSSA area. This command provides the metric for the summary default route, generated by the area border router, into the NSSA or stub area. Use this option only on an area border router that is attached to the NSSA or stub area. Refer to the RFC 3101 for information on NSSA.

Use the no form of this command to remove the assigned default-route cost.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) default-cost <0-16777215>
no area (A.B.C.D|<0-4294967295>) default-cost
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
default-cost	Indicates the cost for the default summary route used for a stub or NSSA area.
<0-16777215>	Stub's advertised default summary cost. The default is 1.

Default

By default, route cost is 1

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example sets the default-cost to 10 for area 1.

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 default-cost 10

(config)#router ospf 100
(config-router)#no area 1 default-cost
```

area filter-list

Use this command to configure a filter to advertise summary routes on an Area Border Router (ABR).

This command suppresses incoming and outgoing summary routes between this area and other areas. You use this command in conjunction with the `prefix-list` and `access-list` commands.

Use the `no` form of this command to remove a filter.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out)
area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out)
no area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out)
no area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out)
```

Parameters

`A.B.C.D`	OSPF area ID as an IPv4 address.
`<0-4294967295>`	OSPF area ID as a decimal value.
`prefix`	Use prefix list to filter summary.
`WORD`	Name of the prefix list.
`access`	Use access list to filter summary.
`WORD`	Name of the access list.
`in`	Filter routes from other areas into this area.
`out`	Filter routes from this area into other areas.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list 1 deny 172.22.0.0
(config)#router ospf 100
(config-router)#area 1 filter-list access 1 in
```

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the no form of this command to remove this designation.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)| stability-
  interval < 0-2147483647>|no-redistribution|default-information-originate (metric
  < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-2>|metric-
  type< 1-2> metric <0-16777214>|)|no-summary}

area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always|never)|
  stability-interval < 0-2147483647>|no-redistribution|default-information-
  originate (metric < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type
  <1-2>|metric-type< 1-2> metric <0-16777214>|)|no-summary}

no area (A.B.C.D|<0-4294967295>) nssa

no area (A.B.C.D|<0-4294967295>) nssa {translator-role|stability-interval|no-
  redistribution |default-information-originate (route-map |) |no-summary}
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
translator-role	
	NSSA-ABR translator role
candidate	Translate NSSA-LSA to Type-5 LSA if router is elected.
never	Do not translate NSSA-LSA to Type-5 LSA.
always	Always translate NSSA-LSA to Type-5 LSA.
stability-interval	
	Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.
<0-2147483647>	
	Stability interval in seconds.
no-redistribution	
	Do not redistribute into the NSSA.
default-information-originate	
	Originate Type-7 default LSA into the NSSA.

`metric`	Specify metric for default routes.
`<0-16777214>`	Specify metric value.
`metric-type`	Specify metric type (see RFC 3101).
`<1-2>`	Specify metric type: 1: Type 1 external route 2: Type 2 external route
`route-map`	OSPF default Route map reference.
`WORD`	Pointer to route-map entries.
`no-summary`	Do not inject inter-area routes into the NSSA.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```

area range

Use this command to summarize OSPF routes at an area boundary. A single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the no parameter with this command to disable this function.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D)
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) advertise
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) not-advertise
area (A.B.C.D|<0-4294967295>) range A.B.C.D A.B.C.D (advertise|non-advertise)
no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D)
no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D)
  (advertise|not-advertise)
```

Parameters

A.B.C.D	Area range prefix or length e.g. X.X.X.X/length
A.B.C.D	Area range prefix e.g. A.B.C.D
<0-4294967295>	OSPF Area ID as a decimal value.
A.B.C.D/M	The area range prefix and length.
advertise	Advertises this range.
not-advertise	Does not advertise this range.

Default

By default, area range is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 range 192.16.0.0/24

(config)#router ospf 100
(config-router)#no area 1 range 192.16.0.0/24
```

area stub

Use this command to define an area as a stub area. There are two stub area router configuration commands: the `stub` and `default-cost` commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area default-cost` command.

Use the `no-summary` parameter with this command to define a totally stubby area. Define an area as a totally stubby area when routers in the area do not need to learn about summary LSAs from other areas.

Use the `no` form of this command to disable this function.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) stub
area (A.B.C.D|<0-4294967295>) stub no-summary
no area (A.B.C.D|<0-4294967295>) stub
no area (A.B.C.D|<0-4294967295>) stub no-summary
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`no-summary`	Stops an ABR from sending summary link advertisements into the stub area.

Default

By default, no stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 stub no-summary
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other non-backbone area.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection. Configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the hello-interval to be the same for all routers attached to a common network. A short hello-interval results in the router detecting topological changes faster but also an increase in the routing traffic. The retransmit-interval is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The transmit-delay is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface. Include the transit area ID and the corresponding virtual link neighbor's router ID in each virtual link neighbor to properly configure a virtual link.

Use the `no` parameter with this command to remove a virtual link.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {authentication (message-
  digest|null|)|authentication-key LINE|message-digest-key <1-255> md5 LINE|dead-
  interval <1-65535>|hello-interval <1-65535>|retransmit-interval <1-
  3600>|transmit-delay <1-3600>}
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {authentication
  (messagedigest| null|)|authentication-key LINE|message-digest-key <1-255> md5
  LINE|deadinterval <1-65535>|hello-interval <1-65535>|retransmit-interval <1-
  3600>|transmit-delay <1-3600>}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D`	Specify IP address of the virtual link neighbor.
`authentication`	Enable authentication on this virtual link
`message-digest`	Cryptographic authentication.
`null`	Null authentication.
`authentication-key`	Set authentication key.
`LINE`	Authentication key ID of 8 characters.
`message-digest-key`	

	Set message digest key.
<1-255>	Set message digest key.
md5	Specify the MD5 key.
LINE	MD5 key.
dead-interval	The interval during which no packets are received and after which the router acknowledges a neighboring router as off-line.
<1-65535>	The interval in seconds. The default is 40 seconds.
hello-interval	The interval the router waits before it sends a hello packet.
<1-65535>	The interval in seconds. The default is 10 seconds.
retransmit-interval	
	The interval the router waits before it retransmits a packet.
<1-3600>	The interval in seconds. The default is 5 seconds.
transmit-delay	The interval the router waits before it transmits a packet.
<1-3600>	The interval in seconds. The default is 1 second
fall-over	Specify fall-over detection.
bfd	Bidirectional Forwarding Detection (BFD)

Default

Default intervals:

Dead interval : 40 seconds

Hello interval: 10 seconds

Retransmit interval: 5 seconds

Transmit delay: 1 second

Command Mode

Router mode

OcNOS version 1.3

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
```

auto-cost reference bandwidth

Use this command to control how OSPF calculates the default metric for the interface.

Use the no form of this command to assign cost based only on the interface bandwidth.

Command Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameters

<1-4294967>	The reference bandwidth in Mbps per second. The default is 100 Mbps.

Default

By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default value for the reference bandwidth is 100Mbps. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#auto-cost reference-bandwidth 50

(config)#router ospf 100
(config-router)#no auto-cost reference-bandwidth
```

bfd all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all interfaces.

Use the no form of this command to disable BFD.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#bfd all-interfaces

(config)#router ospf 100
(config-router)#no bfd all-interfaces
```

capability cspf

Use this command to enable the CSPF (Constrained Shortest Path First) feature for an OSPFv2 or OSPFv3 instance.

Use the `no` parameter with this command to disable CSPF functionality for the OSPFv2 or OSPFv3 instance.

Command Syntax

```
capability cspf
no capability cspf
```

Parameters

None

Default

By default, CSPF functionality for the OSPFv2 or OSPFv3 instance is enabled.

When CSPF is enabled, `disable-better-protection` option is by default enabled for OSPFv2.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability cspf

(config)#router ospf 100
(config-router)#no capability cspf
```

capability lls

Use this command to enable link-local signaling feature on OSPF router.

Use no parameter to disable link-local signaling feature on OSPF router.

Command Syntax

```
capability lls
no capability lls
```

Parameters

None

Default

By default, capability lls is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability lls

(config-router)#no capability lls
```

capability opaque

Use this command to enable opaque-LSAs which are Type 9, 10 and 11 LSAs that deliver information used by external applications.

Use the no form of this command to disable the feature.

Command Syntax

```
capability opaque
no capability opaque
```

Parameters

None

Default

By default, opaque-LSA is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability opaque

(config)#router ospf 100
(config-router)#no capability opaque
```

capability te/traffic-engineering

Use this command to enable traffic engineering feature on OSPF router.

Use no parameter to disable traffic engineering feature on OSPF router.

Command Syntax

```
capability traffic-engineering
capability te
no capability traffic-engineering
no capability te
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#capability traffic-engineering

(config-router)#no capability traffic-engineering
```

capability vrf-lite

Use this command to apply multi-VRF capability to OSPF process or to decouple the PE router from the VPN backbone.

Use no parameter to deny multi-VRF capability to OSPF process or to avoid decoupling the PE router from the VPN backbone.

Command Syntax

```
capability vrf-lite
no capability vrf-lite
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#capability vrf-lite

(config-router)#no capability vrf-lite
```

clear ip ospf

Use this command to clear and restart all OSPF routing processes or a given OSPF routing process.

Command Syntax

```
clear ip ospf (<0-65535>|) process
```

Parameter

<0-65535>	Specify the process ID.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip ospf process
#clear ip ospf 555 process
```

compatible rfc1583

Use this command to restore the method used to calculate summary route costs per RFC.

RFC 1583 specified a method for calculating the metrics for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost. With this change, it is possible that all of the ABRs in an area might not be upgraded to the new code at the same time. This command addresses this issue and allows the selective disabling of RFC 2328 compatibility.

Use the `no` parameter with this command to disable RFC 1583 compatibility.

Command Syntax

```
compatible rfc1583
```

```
no compatible rfc1583
```

Parameters

None

Default

By default, OSPF is RFC 2328 compatible

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#compatible rfc1583

(config)#router ospf 100
(config-router)#no compatible rfc1583
```

debug ospf

Use this command to specify debugging options for OSPF.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|)
debug ospf rib ({interface|redistribute}|)
no debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|)
undebug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|)
no debug all ospf
undebug all ospf
no debug all
no debug ospf rib ({interface|redistribute}|)
undebug all
```

Parameters

`all`	Enable or disable debugging for `ifsm`, `nsfm`, `lsa`, `nsm`, `events`, and `route`.
`bfd`	Debug Bidirectional Forwarding Detection (BFD)
`database-timer`	Debug OSPF rate-limiting values for LSA throttling (see debug ospf database-timer rate-limit)
`events`	Debug OSPF events information (see debug ospf events)
`ifsm`	Debug OSPF Interface State Machine (see debug ospf ifsm)
`lsa`	Debug OSPF Link State Advertisement (see debug ospf lsa)
`nfsm`	Debug OSPF Neighbor State Machine (see debug ospf nfsm)
`nsm`	Debug OSPF NSM information (see debug ospf nsm)
`packet`	Debug OSPF packets (see debug ospf packet)
`route`	Debug OSPF route information (see debug ospf route)
`rib`	Debug OSPF RIB information
`sr`	Debug OSPF segment routing information
`interface`	Debug OSPF RIB interface
`redistribute`	Debug OSPF RIB redistribute

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf all

#debug ospf bfd
#no debug ospf bfd
```

debug ospf database-timer rate-limit

Use this command to log when link-state advertisement (LSA) rate-limiting timers will expire. These messages are logged only when debug ospf lsa `generate` or debug ospf lsa `refresh` is enabled

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf database-timer rate-limit

no debug ospf database-timer rate-limit
undebug ospf database-timer rate-limit
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf database-timer rate-limit
#undebug ospf database-timer rate-limit
```

debug ospf events

Use this command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)

no debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)
undebug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)
```

Parameters

abr	Debug OSPF ABR events.
asbr	Debug ASBR events.
lsa	Debug LSA events.
nssa	Debug NSSA events.
os	Debug OS interaction events.
router	Debug other router events.
vlink	Debug virtual link events.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf event abr
#debug ospf event asbr
#debug ospf event lsa
#no debug ospf event nssa
#debug ospf event os
#debug ospf event router
#debug ospf event vl
```

debug ospf ifsm

Use this command to specify debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf ifsm ({events|status|timers}|)

no debug ospf ifsm ({events|status|timers}|)
undebug ospf ifsm ({events|status|timers}|)
```

Parameters

`events`	Debug IFSM event information
`status`	Debug IFSM status information
`timers`	Debug IFSM timer information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf ifsm events
#debug ospf ifsm status
#debug ospf ifsm timers
```

debug ip ospf lfa

Use this command to specify the debugging options for OSPFv2 Loop-free Alternate path

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ip ospf lfa
no debug ip ospf lfa
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf lfa
```

debug ip ospf redist

Use this command to display debugging option for OSPF redistribute information

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ip ospf redist (detail|terse|)
no debug ip ospf redist (detail|terse|)
```

Parameters

`detail`	Debug OSPF redistribute detail information
`terse`	Debug OSPF redistribute summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf redistribute detail
```

debug ip ospf retransmission

Use this command to display debug logs of OSPF retransmission information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ip ospf retransmission
no debug ip ospf retransmission
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf retransmission
```

debug ospf lsa

Use this command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf lsa ({flooding|generate|install|maxage|refresh}|)

no debug ospf lsa ({flooding|generate|install|maxage|refresh}|)
undebug ospf lsa ({flooding|generate|install|maxage|refresh}|)
```

Parameters

`flooding`	Debug LSA flooding.
`generate`	Debug LSA generation.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf lsa refresh
#debug ospf lsa flooding
#debug ospf lsa install
#debug ospf lsa maxage
#debug ospf lsa generate
```

debug ospf nfsm

Use this command to specify debugging options for OSPF Neighbor Finite State Machines (NFSMs).

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf nfsm ({events|status|timers}|)

no debug ospf nfsm ({events|status|timers}|)
undebug ospf nfsm ({events|status|timers}|)
```

Parameters

events	Debug NFSM event information
status	Debug NFSM status information
timers	Debug NFSM timer information

Command Mode

Privileged Exec mode Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf nfsm events
#no debug ospf nfsm timers
```

debug ospf nsm

Use this command to specify debugging options for OSPF NSM information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf nsm ({interface|redistribute}|)

no debug ospf nsm ({interface|redistribute}|)
undebug ospf nsm ({interface|redistribute}|)
```

Parameters

`interface`	Debug NSM interface information.
`redistribute`	Debug NSM redistribute information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The `debug ospf nsm` command enables the display of debug information related to NSM.

```
#debug ospf nsm interface
#no debug ospf nsm redistribute
```

debug ospf packet

Use this command to specify debugging options for OSPF packets.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)

no debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
undebug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPF hello packets.
`dd`	Debug OSPF database.
`ls-request`	Debug OSPF link state requests.
`ls-update`	Debug OSPF link state updates.
`ls-ack`	Debug OSPF link state acknowledgments.
`send`	Debug OSPF sent packets.
`recv`	Debug OSPF received packets.
`detail`	Debug OSPF detailed information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf packet detail
#debug ospf packet dd send detail
#no debug ospf packet ls-request recv detail
```

debug ospf rib

Use this command to display debug information about the interaction between the OSPF process and the Routing Information Base (RIB).

Use no parameter of this command to disable debugging output.

Command Syntax

```
debug ospf rib ({interface|redistribute}|)
no debug ospf rib ({interface|redistribute}|)
debug ip ospf ({client|redistribute}|)
no debug ip ospf ({client|redistribute}|)
undebug ospf rib ({interface|redistribute}|)
```

Parameters

`interface`	Debug RIB interface information.
`redistribute`	Debug RIB redistribute information.
`client`	Debug RIB client information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ospf rib interface
#no debug ospf rib redistribute
```

debug ospf route

Use this command to debug route calculation. Use this command without parameters to turn on all the options.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf route ({ase|ia|install|spf}|)
no debug ospf route ({ase|ia|install|spf}|)
undebug ospf route ({ase|ia|install|spf}|)
```

Parameters

ase	Debug OSPF external route calculation.
ia	Debug OSPF Inter-Area route calculation.
install	Debug OSPF route installation.
spf	Debug OSPF SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf route
#no debug ospf route ia
#debug ospf route install
```

default-information originate

Use this command to create a default external route into an OSPF routing domain.

Use the no parameter with this command to disable this feature.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Command Syntax

```
default-information originate
default-information originate {metric <0-16777214>|metric-type (1|2)|?route-map
  WORD|always}
no default-information originate
no default-information originate {metric|metric-type|?route-map|always}
```

Parameters

`always`	Used to advertise the default route regardless of whether there is a default route.
`metric`	Sets the OSPF metric used in creating the default route.
`<0-16777214>`	Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol.
`metric-type`	The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).
`1`	Sets OSPF External Type 1 metric.
`2`	Sets OSPF External Type 2 metric (default).
`route-map`	Route map.
`WORD`	Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 10.

The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 Sets OSPF External Type 2 metric.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-information originate always metric 23 metric-type 2
route-map myinfo

(config)#router ospf 100
(config-router)#no default-information originate metric metric-type route-map
```

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the no parameter with this command to return to the default state.

Command Syntax

```
default-metric <1-16777214>


no default-metric
no default-metric <1-16777214>
```

Parameters

<1-16777214>	Default metric value.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-metric 100
```

distance

Use this command to set OSPF administrative distances.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 255 means that the routing information source cannot be trusted and should be ignored.

Use the no form of this command to restore the default value (110).

Command Syntax

```
distance <1-255>
distance <1-255> A.B.C.D/M (WORD|)
distance ospf {intra-area <1-255>|inter-area <1-255>|external <1-255>}
no distance <1-255>
no distance <1-255> A.B.C.D/M (WORD|)
no distance ospf {intra-area |inter-area |external}
```

Parameters

<1-255>	Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.
intra-area	Routes within an area.
<1-255>	Distance for all routes within an area
inter-area	Routes from one area to another area.
<1-255>	Distance for all routes from one area to another area.
external	Routes from other routing domains learned by redistribution.
<1-255>	Distance for routes from other routing domains learned by redistribution.
A.B.C.D/M	Distance for routes to prefixes whose nexthop matches this address.
WORD	Name of access list to apply to route updates.

Default

By default, distance for each type of route (intra-, inter-, or external) is 110

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the no parameter with this command to disable this function.

Command Syntax

```
distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|))
distribute-list WORD in
no distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|))
no distribute-list WORD in
```

Parameters

`WORD`	Specify the name of the access list.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF process.
`<1-65535>`	Specify OSPF process ID <1-65535>. If not specified, this command redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list `list1` (network 172.10.0.0).

```
#configure terminal
(config)#access-list list1 permit 172.10.0.0
(config)#router ospf 100
(config-router)#distribute-list list1 out bgp
```

```
(config-router)#redistribute bgp
```

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv2.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in database summary list is the same as or less recent than the listed LSA in the database description packet received from the neighbor.

Use the no form of this command to disable database summary list optimization.

Command Syntax

```
enable db-summary-opt
```

```
no enable db-summary-opt
```

Parameters

None

Default

By default, database summary list optimization for OSPFv2 is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPF interfaces.

Use the no parameter with this command to disable fast rerouting.

Command Syntax

```
fast-reroute keep-all-paths
no fast-reroute keep-all-paths
```

Parameters

None

Defaults

By default, fast rerouting is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
(config-router)#fast-reroute keep-all-paths
```

fast-reroute terminate-hold-on interval

Use this command to set the delay of primary route installation (to avoid micro loop) after a failover.

Use the no form of this command to set the termination hold-on timer to its default value (600 milliseconds).

Command Syntax

```
fast-reroute terminate-hold-on interval <100-100000>
no fast-reroute terminate-hold-on interval
```

Parameters

<100-100000>Hold on interval in milliseconds

Defaults

600 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 1
(config-router)#fast-reroute terminate-hold-on interval 7000
(config-router)#no fast-reroute terminate-hold-on interval
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path. The tie-breaker value is used to select an LFA FRR route when multiple LFA FRR routes are available for the same primary route.

Use the no form of this command to set the tie-break preference value for a protection type to its default value as shown in Table 1-133.

To set all types of repair paths to their default priorities, do not specify a repair path with the no form of this command.

Command Syntax

```
fast-reroute tie-break (primary-path|interface-disjoint|node-protecting|broadcast-
  interface-disjoint|downstream-path|secondary-path) index <1-255>

no fast-reroute tie-break

no fast-reroute tie-break (primary-path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint|downstream-path|secondary-path)
```

Parameters

`primary-path` Use a path from the Equal-Cost Multipath Path (ECMP) set. An ECMP found during the primary shortest path first (SPF) repair might not be desirable in networks where traffic exceeds the capacity of any single link.

`interface-disjoint`

Prefer a backup path that uses a different interface than the interface used to reach destination via the primary path.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path. This ensures complete traffic protection even if the primary next-hop router fails.

`broadcast-interface-disjoint`

Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.

`downstream-path`

Prefer a backup path to the destination which satisfies the downstream condition where the path cost to reach the destination from the LFA next hop is less than the path cost to the destination from the self node via primary next hop:

Distance_opt(N, D) < Distance_opt(S, D)

This might result in lost traffic, but prevents looping.

`secondary-path` Prefer a non-ECMP backup path.

`index` Tie break priority. A lower value has higher preference.

`<1-255>` Range of priority values.

Defaults

primary-path	20
interface-disjoint	60
node-protecting	30
broadcast-interface-disjoint	70
secondary-path	255
downstream-path	90

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
(config-router)#fast-reroute tie-break interface-disjoint index 1
```

host area

Use this command to configure a stub host entry belonging to a particular area.

Using this command, you can advertise specific host routes in the router-LSA as stub link. Since stub host belongs to the specified router, specifying cost is not important.

Use the no form of this command to remove the host area configuration.

Command Syntax

```
host A.B.C.D area (A.B.C.D|<0-4294967295>)
host A.B.C.D area (A.B.C.D|<0-4294967295>) cost <0-65535>
no host A.B.C.D area (A.B.C.D|<0-4294967295>)
no host A.B.C.D area (A.B.C.D|<0-4294967295>) cost (<0-65535>|)
```

Parameters

A.B.C.D	Specify IP address of the host.
area	Set the OSPF area ID
A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
cost	Specify cost for stub host entry.
<0-65535>	Specify cost for stub host entry.

Default

No host entry is configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#host 172.16.10.100 area 1
(config-router)#host 172.16.10.101 area 2 cost 10
```

ip ospf authentication

Use this command to send and receive OSPF packets with the specified authentication method on the current interface.

Use the no parameter with this command to disable the authentication.

Command Syntax

```
ip ospf authentication (null|message-digest|)
ip ospf A.B.C.D authentication (null|message-digest|)
no ip ospf (A.B.C.D|) authentication
```

Parameters

A.B.C.D	The IP address of the interface.
null	Use no authentication.
message-digest	Use message digest authentication.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In this example, interface eth0 is configured to have no authentication. This will override any text or MD5 authentication configured on this interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication null
```

ip ospf authentication-key

Use this command to specify an OSPF authentication password for neighboring routers.

This command creates a password (key) that is inserted into the OSPF header when OcNOS originates packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area with the `area authentication` command.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Use the `no` parameter with this command to remove an OSPF authentication password.

Command Syntax

```
ip ospf (A.B.C.D|) authentication-key WORD
ip ospf (A.B.C.D|) authentication-key 0 WORD
no ip ospf (A.B.C.D|) authentication-key
```

Parameters

`A.B.C.D`	The IP address of the interface.
`authentication-key`	
	Specify the authentication password.
`WORD`	Specify the OSPF Encrypted password (key) of 8 bytes.
`0`	Specify the unencrypted password (key).
`WORD`	Specify the OSPF password (key) up to maximum 8 characters.

Default

By default, no password used when exchanging OSPF routing data

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, an authentication key `test` is created on interface `eth0` in area `0`. Note that first authentication is enabled for area `0`.

```
#configure terminal
(config)#router ospf 100
(config-router)#network 10.10.10.0/24 area 0
(config-router)#area 0 authentication
(config-router)#exit
(config)#interface eth0
(config-if)#ip ospf 3.3.3.3 authentication-key test
```

ip ospf bfd

Use this command to enable Bidirectional Forwarding Detection (BFD).

Use this command with either the `no` or `disable` parameter to disable BFD.

Command Syntax

```
ip ospf bfd (disable|)
no ip ospf bfd (disable|)
```

Parameters

`disable`	Specify to disable BFD.

Default

By default, ip ospf bfd is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf bfd
```

ip ospf cost

Use this command to explicitly specify the cost of the link-state metric in a router-LSA.

The interface cost indicates the overhead required to send packets across an interface. This cost is stated in the Router-LSA's link. The cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). Use this command to set the cost manually.

Use the `no` parameter with this command to reset the cost to its default value.

Command Syntax

```
ip ospf (A.B.C.D|) cost <1-65535>
no ip ospf (A.B.C.D|) cost
```

Parameters

`A.B.C.D`	The IP address of the interface.
`<1-65535>`	Specify the link-state metric.

Default

By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). The default cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the cost as 10 on interface `eth0` for IP address 10.10.10.50.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf 10.10.10.50 cost 10
```

ip ospf database-filter

Use this command to turn on the LSA database-filter for a particular interface.

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use this command to block flooding of LSAs over specified interfaces.

Use the no parameter with this command to turn off the filter.

Command Syntax

```
ip ospf (A.B.C.D|) database-filter all out
no ip ospf (A.B.C.D|) database-filter
```

Parameters

A.B.C.D	The IP address of the interface.

Default

Disabled, all outgoing LSAs are flooded to the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf database-filter all out
```

ip ospf dead-interval

Use this command to set the interval during which the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

Use the no parameter with this command to return to the default time. If you have configured this command specifying the IP address of the interface and want to remove the configuration, use the no parameter with the specified IP address (`no ip ospf dead-interval A.B.C.D`).

Command Syntax

```
ip ospf (A.B.C.D|) dead-interval <1-65535>
no ip ospf (A.B.C.D|) dead-interval
```

Parameters

`A.B.C.D`	The IP address of the interface.
`dead-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows configuring dead-interval for 10 seconds on eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf dead-interval 10
```

ip ospf disable

Use this command to completely disable OSPF packet processing on an interface.

This command overrides the network command.

Use the no option with this command to return to the default setting.

Command Syntax

```
ip ospf disable all
no ip ospf disable all
```

Parameters

None

Default

By default, this feature is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf disable all
```

ip ospf fast-reroute per-prefix candidate disable

Use this command to prohibit the interface from being used as the next hop in a repair path.

Use the no option with this command to use the interface as the next hop in a repair path.

Command Syntax

```
ip ospf fast-reroute per-prefix candidate disable
no ip ospf fast-reroute per-prefix candidate disable
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf fast-reroute per-prefix candidate disable
```

ip ospf flood-reduction

Use this command to enable flood reduction on an interface. When this command is configured, an LSA sent out on the interface is set with the DNA bit in the LSA age field. The LSA is not refreshed every refresh interval if there is no change in LSA. Only changed LSAs are sent out on the interface

Use the no option with this command to disable flood reduction on an interface.

Command Syntax

```
ip ospf flood-reduction
no ip ospf flood-reduction
```

Parameters

None

Default

By default, flood reduction on an interface is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf flood-reduction

(config-if)#no ip ospf flood-reduction
```

ip ospf hello-interval

Use this command to specify the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but results in more routing traffic.

Use the no parameter with this command to return to the default time.

Command Syntax

```
ip ospf (A.B.C.D|) hello-interval <1-65535>
no ip ospf (A.B.C.D|) hello-interval
```

Parameters

A.B.C.D	The IP address of the interface.
hello-interval	Specify the interval.
<1-65535>	Specify the interval in seconds.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the hello-interval for 3 seconds on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf hello-interval 3
```

ip ospf multi-area

Use this command to enable multi-area adjacency on point-to-point network and other network types. Multi-area adjacency establishes adjacency between the Area Border Routers (ABRs). The interface of the ABR where this command is configured, shall be associated with multiple areas.

Use the no parameter to disable multi-area adjacency on the given interface on point-to-point network.

Command Syntax

```
ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)(neighbor A.B.C.D |)
no ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)
```

Parameters

<0-65535>	OSPF process ID.
A.B.C.D	OSPF area ID in IP address format.
<0-4294967295>	OSPF area ID as a decimal value.
A.B.C.D	Neighbor IP address.

Default

By default, multi-area adjacency is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf 0 multi-area 1

(config-if)# no ip ospf 0 multi-area 1
```

ip ospf message-digest-key

Use this command to register an MD5 key for OSPF authentication.

Use the no parameter with this command to remove an MD5 key.

Message Digest Authentication is cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that is appended to the packet.

Use this command for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever you add a new one. This prevents the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Command Syntax

```
ip ospf (A.B.C.D|) message-digest-key <1-255> md5 LINE
no ip ospf (A.B.C.D|) message-digest-key <1-255>
```

Parameters

A.B.C.D	IPv4 address of the interface.
message-digest-key	
	Specify a key ID.
<1-255>	Specify a key ID.
md5	Specify a key (password).
LINE	Specify the OSPF password (1-16 characters).

Default

By default, MD5 key for OSPF authentication is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows OSPF authentication on the interface eth0 when IP address has not been specified.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication message-digest
(config-if)#ip ospf message-digest-key 1 md5 yourpass
```

The following example shows OSPF authentication on the interface eth0 for the IP address 1.1.1.1. (If the interface has two IP addresses assigned-- 1.1.1.1 & 2.2.2.2, OSPF authentication will be enabled only for the IP address 1.1.1.1)

```
(config)#interface eth0
(config-if)#ip ospf 1.1.1.1 authentication message-digest
(config-if)#ip ospf 1.1.1.1 message-digest-key 2 md5 yourpass
```

ip ospf mtu

Use this command to set MTU size for OSPF to construct packets based on this value. Whenever OSPF constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value overriding the actual interface MTU size.

This command does not configure the MTU settings in the kernel. OSPF does not recognize MTU size changes made in the kernel until the MTU size is updated through this command.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf mtu <576-65535>
no ip ospf mtu
```

Parameters

`mtu`	Specify an MTU size.
`<576-65535>`	Specify an MTU size.

Default

By default, OSPF uses interface MTU derived from the kernel.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf mtu 1480
```

ip ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the no form of this command to make OSPF check the MTU size during DD exchange.

Command syntax

```
ip ospf (A.B.C.D|) mtu-ignore
no ip ospf (A.B.C.D|) mtu-ignore
```

Parameters

A.B.C.D	IP address of the interface.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-router)#ip ospf mtu-ignore
```

ip ospf network

Use this command to set the OSPF network type.

Use the no parameter with this command to return to the default value.

Command Syntax

```
ip ospf network (broadcast|non-broadcast|point-to-multipoint|point-to-point)
ip ospf network point-to-multipoint non-broadcast
no ip ospf network
```

Parameters

`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`non-broadcast`	Sets the network type to NBMA.
`point-to-point`	Sets the network type to point-to-point.

Default

By default, OSPF network type is broadcast

Command Mode

interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the network to `point-to-point` type on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf network point-to-point
```

ip ospf priority

Use this command to set the router priority to determine the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the no parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) priority <0-255>
no ip ospf (A.B.C.D|) priority
```

Parameters

A.B.C.D	The IP address of the interface.
priority	Specify the router priority of the interface.
<0-255>	Specify the router priority of the interface. The default value is 1.

Default

By default, ip ospf priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the OSPF priority value to 3 on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf priority 3
```

ip ospf retransmit-interval

Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. If the router does not receive an acknowledgement during the retransmit interval, it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) retransmit-interval <5-65535>
no ip ospf (A.B.C.D|) retransmit-interval
```

Parameters

`A.B.C.D`	The IPv4 address of the interface.
`retransmit-interval`	Specify the interval.
`<5-65535>`	Specify the interval in seconds.

Default

By default, retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the `ospf retransmit interval` to 6 seconds on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf retransmit-interval 6
```

ip ospf transmit-delay

Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Use the no parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) transmit-delay <1-65535>
no ip ospf (A.B.C.D|) transmit-delay
```

Parameters

`A.B.C.D`	The IPv4 address of the interface.
`transmit-delay`	Specify the time to transmit a link-state update.
`<1-65535>`	Specify the time in seconds to transmit a link-state update.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the OSPF transmit delay time to 3 seconds on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf transmit-delay 3
```

log-adjacency-changes

Use this command for the router to send a SYSLOG message when an OSPF neighbor goes up or down.

Use no parameter of this command to stop sending SYSLOG message.

Command Syntax

```
log-adjacency-changes (detail|)
no log-adjacency-changes (detail|)
```

Parameters

`detail`	Sends a SYSLOG message for each state change, not just when a neighbor goes up or down.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#log-adjacency-changes
(config-router)#log-adjacency-changes detail
(config-router)#no log-adjacency-changes
(config-router)#no log-adjacency-changes detail
```

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Use the no option with this command to remove the limit.

Command Syntax

```
max-concurrent-dd <1-65535>
no max-concurrent-dd
```

Parameters

`<1-65535>`	Specify the number of DD processes.

Default

By default, max concurrent dd value is 64

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ospf 100
(config-router)#max-concurrent-dd 4
```

maximum-area

Use this command to configure the maximum number of OSPF areas.

Use the `no` parameter with this command to disable the limit.

Command Syntax

```
maximum-area <1-4294967294>
no maximum-area
```

Parameters

`<1-4294967294>` Specify the maximum number of OSPF areas.

Default

By default, ospf maximum area is 4294967294

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#maximum-area 5
```

neighbor

Use this command to configure OSPF routers interconnecting to NBMA (Non-Broadcast Multi-Access) networks. Include one neighbor entry for each known non-broadcast network neighbor. Configure the neighbor address on the primary address of the interface.

Use the no parameter with this command to remove a configuration.

Command Syntax

```
neighbor A.B.C.D
neighbor A.B.C.D (priority <0-255>|poll-interval <1-2147483647>)
no neighbor A.B.C.D
no neighbor A.B.C.D {priority (<0-255>|)|poll-interval (<1-2147483647>|)}
```

Parameters

A.B.C.D	Specify the interface IP address of the neighbor.
priority	Specify the router priority of the non-broadcast neighbor associated with the specified IP address.This parameter does not apply to point-to-multipoint interfaces.
<0-255>	Specify the router priority value of the non-broadcast neighbor associated with the specified IP address.
poll-interval	The reduced rate at which routers continue to send hello packets when a neighboring router has become inactive.
<1-2147483647>	Dead neighbor polling interval in seconds. Set this value much larger than hello interval.

Default

The default priority is 0 and polling interval is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows neighbor configured with a priority value and poll interval time.

```
#configure terminal
(config)#router ospf 100
(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
```

network

Use this command to enable OSPF routing with a specified area ID (and optionally an instance ID) on interfaces with IP addresses that match the specified network address.

OSPF routing is enabled per IPv4 subnet basis. You define the network address using the prefix length or a subnet mask.

Use the `no` parameter with this command to disable OSPF routing on the interfaces.

Command Syntax

Network address defined using the prefix length:

```
network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
no network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
```

Network address defined using subnet mask:

```
network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
no network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
```

Parameters

`A.B.C.D/M`	IPv4 network address with prefix length.
`A.B.C.D`	IPv4 network address.
`A.B.C.D`	Subnet mask where the bits on left side are set to 1 to represent the network part and the bits on the right side are set to 0 to represent the host part.
`area`	OSPF area ID
`A.B.C.D`	OSPF area ID in IPv4 address format.
`<0-4294967295>`	OSPF area ID as a decimal value.
`instance-id`	Instance ID
`<0-255>`	Instance ID value.

Default

No network area is configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following the use of the `network` command with OSPF multiple-instance support disabled.

```
#configure terminal
(config-router)#network 10.0.0.0/8 area 3
(config-router)#network 10.0.0.0/8 area 1.1.1.1
```

The following shows the use of the network command with OSPF multiple-instance support enabled.

```
(config)#router ospf 100
(config-router)#network 10.0.0.0/8 area 3 instance-id 4
```

ospf abr-type

Use this command to set an OSPF Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax

```
ospf abr-type (cisco|ibm|standard)
no ospf abr-type (cisco|ibm|standard|)
```

Parameters

`cisco`	Specify an alternative ABR using Cisco implementation. This is the default ABR type.
`ibm`	Specify an alternative ABR using IBM implementation.
`standard`	Specify a standard ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf abr-type ibm
```

ospf flood-reduction

Use this command to Enable flood reduction on all OSPF interface. When this command is configured, an LSA sent out on the OSPF interface is set with the DNA bit in the LSA age field. If there is no change in LSA, it is not refreshed every refresh interval. LSAs are sent out on the interface only if there is a change in an LSA

Use the no option with this command to disable flood reduction on all OSPF interfaces.

Command Syntax

```
ospf flood-reduction
no ospf flood-reduction
```

Parameters

None

Default

By default, flood reduction on all OSPF interfaces is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf flood-reduction

(config-router)#no ospf flood-reduction
```

ospf router-id

Use this command to specify a router ID for the OSPF process.

Configure each router with a unique router ID. In an OSPF router process which has active neighbors, a new router ID is used at the next reload or when you start the OSPF manually.

Use the no parameter with this command to force OSPF to use the previous router ID.

Command Syntax

```
ospf router-id A.B.C.D
router-id A.B.C.D

no ospf router-id
no router-id (A.B.C.D|)
```

Parameters

A.B.C.D	Specify the router ID in IPv4 address format.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows a specified router ID 2.3.4.5.

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf router-id 2.3.4.5
```

overflow database

Use this command to limit the maximum number of LSAs that can be supported by the OSPF instance.

Use the no parameter with this command to have an unlimited number of LSAs.

Command Syntax

```
overflow database <0-4294967294> (hard|soft|)
no overflow database
```

Parameters

<0-4294967294>	The maximum number of LSAs
hard	Shutdown occurs if the number of LSAs exceeds the specified value.
soft	Warning message appears if the number of LSAs exceeds the specified value.

Default

No default value is specified. unlimited number of LSAs.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the database overflow to 5 and shutting down in that event.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database 5 hard
```

overflow database external

Use this command to limits the number of AS-external-LSAs a router can receive once it is in the wait state.

Use the no parameter with this command to revert to default.

Command Syntax

```
overflow database external <0-2147483647> <0-65535>
no overflow database external
```

Parameters

<0-2147483647>	The maximum number of LSAs. This value should be the same on all routers in the AS.
<0-65535>	The number of seconds the router waits before trying to exit the database overflow state. If this parameter is 0, the router exits the overflow state only after an explicit administrator command.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is unlimited.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the maximum number of LSAs to 5 and the time to recover from overflow state to be 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database external 5 3
```

passive-interface

Use this command to suppress sending Hello packets on all interfaces or on a specified interface.

This command configures OSPF on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPF does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the no form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Command Syntax

```
passive-interface IFNAME
passive-interface (IFNAME A.B.C.D |)
no passive-interface IFNAME
no passive-interface (IFNAME A.B.C.D |)
```

Parameters

`IFNAME`	The name of the interface.
`A.B.C.D`	IP address of the interface.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is 100000.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#passive-interface eth0
```

redistribute

This command redistributes routes from a routing protocol, static route, and kernel route into an OSPF routing table.

Use the no parameter with this command to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|)) {metric <0-
  16777214>|metric-type (1|2)|?route-map WORD|tag <0-4294967295>}
no redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|))
  metric|metric-type|?route-map|tag}
```

Parameters

kernel	Specify kernel routes.
connected	Specify connected routes.
static	Specify static routes.
rip	Specify RIP routes.
bgp	Specify BGP routes.
isis	Specify IS-IS routes.
ospf	Specify OSPF process.
<1-65535>	Specify an OSPF process ID to redistribute a particular OSPF instance into another OSPF instance. If not specified, this command redistribute OSPF instance with process ID 0.
metric	Specify the external metric.
<0-16777214>	Specify the external metric.
metric-type	Specify the external metric-type (see RFC 3101):
1	Set OSPF External Type 1 metrics.
2	Set OSPF External Type 2 metrics.
route-map	Specify a route map reference.
WORD	Specify name of the route-map.
tag	Tag value to use as a “match” value for controlling redistribution via route maps
<0-4294967295>	Specify the route tag.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#redistribute bgp metric 12
```

The following example shows redistributing OSPF instance 2 into OSPF instance 1.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2
```

The following example shows redistributing OSPF instance 2 into OSPF instance 1, with an external metric of 10, metric type 1, a route-map named rmp1, and an external route tag of 3.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2 metric 10 metric-type 1 route-map rmp1 tag
3
```

router ospf

Use this command to enter router mode and to configure an OSPF routing process.

Specify the process ID to configure multiple instances of OSPF. When running a single instance of OSPF, you do not need to specify a process ID.

Use the no parameter with this command to terminate an OSPF routing process.

Command Syntax

```
router ospf
router ospf <1-65535>

no router ospf
no router ospf <1-65535>
```

Parameters

<1-65535>	Process ID; should be unique for each routing process.

Default

No routing process defined

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the use of the `router ospf` command to enter router mode. Note the change in the prompt.

```
#configure terminal
(config)#router ospf 100
(config-router)#
```

show debugging ospf

Use this command to display the set OSPF debugging option.

Command Syntax

```
show debugging ospf
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show debugging ospf` command. Some lines in this output wrap around, they might not wrap around in the actual display.

```
#show debugging ospf
OSPF debugging status:
  OSPF packet Link State Update debugging is on
  OSPF all events debugging is on
```

show ip ospf

Use this command to display general information about all OSPF routing processes.

Command Syntax

```
show ip ospf (<0-65535>|)
```

Parameters

<0-65535>	The ID of the router process for which information will be displayed. If this parameter is specified, only the information for the specified routing process is displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 4.1.1.1
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 5. Checksum 0x010632
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 5
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 0
 Number of areas attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:47.558 ago
```

```
        SPF algorithm executed 2 times
        Number of LSA 1. Checksum 0x0041e0
```

OSPF Routing Process Fields

Table 1-133 explains the routing process fields.

Table 1-133: show ip ospf output details

Field	Description
Routing Process with ID	OSPF process identifier and router identifier.
Process is not up	OSPF process is not running.
Process uptime is	OSPF process running time.
Process bound to VRF	VRF name
Router is in Graceful Restart	When in graceful restart.
Router is in Restart Signaling	When in restart signalling.
Bidirectional Forwarding Detection is configured	When BFD is enabled.
Conforms to RFC2328, and RFC1583 Compatibility flag is enabled	RFC compatibility.
Supports only single TOS (TOS0) routes	OSPF TOS-based routing was never deployed.
Supports opaque LSA	When opaque LSAs are supported.
Do not support Restarting	When restart is not supported.
Supports Graceful Restart	Method of restart in process.
Supports Restart Signaling	Method of restart in signaling process.
Connected to MPLS VPN Super backbone	VRF is enabled and the process is connected to the MPLS VPN backbone.
This router is an ABR, ABR Type is	Type of ABR: Standard (RFC2328) Alternative Cisco (RFC3509) Alternative IBM (RFC3509) Alternative Shortcut
This router is an ASBR (injecting external routing information)	Type of router function in the process.
SPF schedule delay initial	Initial SPF schedule delay.
SPF schedule delay min	Minimum delay between receiving a change to SPF calculation.
SPF schedule delay max	Maximum delay between receiving a change to SPF calculation.
Refresh timer	LSA refresh interval.
Number of incoming current DD exchange neighbors	Incoming neighbor Database Descriptors and maximum concurrent DDs.

Table 1-133: show ip ospf output details (Continued)

Field	Description
Number of outgoing current DD exchange neighbors	Outgoing neighbor Database Descriptors and maximum concurrent DDs.
Initial LSA throttle delay	Initial delay for the generation of LSAs.
Minimum hold time for LSA throttle	Minimum hold time between generation of the same LSA.
Maximum wait time for LSA throttle	Maximum wait time between generation of the same LSA.
Minimum LSA arrival	Minimum time between reception of new LSAs during flooding.
Number of external LSA	Number of AS external LSAs and checksum.
Number of opaque AS LSA	Number of AS opaque LSAs and checksum.
Number of non-default external LSA	For database overflow, number of non-default external LSAs.
External LSA database is unlimited	When the external LSA database is unlimited.
External LSA database limit	Maximum number of LSAs in database.
Exit database overflow state interval is	Exit database overflow state interval.
Exit database overflow state interval is not configured	When the exit database overflow state interval is not set.
OSPF is [not] in database overflow state now	Whether OSPF is in database overflow state now.
Next attempt to exit database overflow state in	How long until OSPF tries to exit the database overflow state.
LSDB database overflow limit	Maximum number of LSAs that can be supported by the OSPF instance.
LSDB exceed overflow limit	Whether OSPF is exceeding the maximum number of LSAs.
Number of LSA originated	LSAs originated by the OSPF instance.
Number of LSA received	LSAs received by the OSPF instance.
Number of areas attached to this router	As stated
Next fields are repeated for each area	As stated
Area	Area identifier.
(BACKBONE)	Area is a backbone.
no-summary	Area is a stub and does no import summaries.
(Inactive)	Area is not active.
Number of interfaces in this area is	Number of interfaces in this area.
Number of fully adjacent neighbors in this area	As stated.
Number of fully adjacent virtual neighbors through this area	As stated.

Table 1-133: show ip ospf output details (Continued)

Field	Description
Area has no authentication	Area does not use authentication.
Area has simple password authentication	Area uses password authentication.
Area has message digest authentication	Area uses MD5 authentication.
SPF algorithm last executed	As stated.
SPF algorithm executed	As stated.
Number of LSA	Number of LSAs in area link-state database and checksum.
End of area field	As stated.
NSSA Translator Role is	candidate: Translate Type-7 LSAs to Type-5 if router is elected. never: Do not translate Type-7 LSAs to Type-5. always: Always translate Type-7 LSAs to Type-5.
NSSA Translator State is	disabled: Router is not a border router. enabled: Router is a border router. elected: Router has been elected to be an NSSA translator.
Stability Interval	If an elected translator determines its services are no longer required, how long it continues to perform its services.
Number of NSSA Translator Events	As stated.
Shortcutting mode	Shortcut ABR that installs inter-area routes through non-backbone areas if non-backbone paths are really better: Default Enabled Disabled
S-bit consensus	Whether other ABR agrees on S-bit: ok no
Dste Status	Whether DSTE is enabled or disabled.

show ip ospf border-routers

Use this command to display the ABRs and ASBRs for OSPF instances.

Command Syntax

```
show ip ospf (<0-65535>|) border-routers
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip ospf border-routers` command.

```
#show ip ospf border-routers
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, eth0, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, eth1, ABR, ASBR, Area 0.0.0.0
```

Border Router Fields

Table 1-134 explains the border router fields.

Table 1-134: border router output details

Field	Description
Code	i: Intra-area route I: Inter-area route
Router ID	Router identifier of the destination
Cost	Cost of using this route.
via	Next hop IP address toward the destination.
is directly connected	Destination is directly connected.
Interface	Outgoing interface name.
Type	Router type of the destination: ABR or ASBR.
through Transit Area	Next hop is an area that carries traffic that neither originates nor terminates in the area itself.
Area	Area identifier from which this route was learned.
Transit	Area is a transit area.

show ip ospf database brief

Use this command to display a summary of the OSPF database.

Command Syntax

```
show ip ospf database (self-originate|max-age|adv-router A.B.C.D|)
show ip ospf <0-65535> database(self-originate|max-age|adv-router A.B.C.D|)
```

Parameters

`self-originate`	Self-originated link states.
`max-age`	LSAs which have reached the maximum age (3600 seconds).
`A.B.C.D`	IPv4 address of the advertising router.
`<0-65535>`	ID of the router process

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf database
       OSPF Router process 100 with ID (100.100.100.72)
                Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum  Link count
10.100.12.57    10.100.12.57     930  0x80000003 0x90de 2
100.100.100.72  100.100.100.72   933  0x80000004 0x7592 2
                Net Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum
10.100.10.72    100.100.100.72   933  0x80000001 0x0bef
                Summary Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum  Route
10.60.0.0       10.100.12.57     928  0x80000001 0x5108 10.60.0.0/24
71.87.120.0     10.100.12.57     928  0x80000001 0xc2c5 71.87.120.0/24
127.0.0.1       10.100.12.57     928  0x80000001 0x23fb 127.0.0.1/32
```

OSPF Database Fields

Table 1-135 explains the fields for each database entry.

Table 1-135: ospf database output details

Field	Description
Link ID	The meaning of this field depends on the type of Link-State Advertisement (LSA). Type 1: Router LSA (depends on the type of network to which the router connects): Point-to-point network: neighbor's router ID. Transit network: IP address of the designated router's interface. Stub network: IP network or subnet address Virtual link: Neighbor's Router ID. Type 2: Network LSA: The IP address of the designated router's interface. Type 3: Summary LSA: The IP address of the network or subnet being advertised.
ADV Router	The ID of the router advertising the LSA.
Age	The age of the LSA.
Seq#	The sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
CkSum	The fetch checksum of the complete LSA except the Age field.
Link count	Total number of links.
Route	Summary prefix address.

show ip ospf database detail

Use this command to display details of the OSPF database.

Command Syntax

```
show ip ospf database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) (self-originate|adv-router A.B.C.D|)
show ip ospf <0-65535> database (asbr-summary|external|network|router|summary)
  (self-originate|adv-router A.B.C.D|)
show ip ospf database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|)
show ip ospf <0-65535> database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|)
```

Parameters

`<0-65535>`	The ID of the router process for which information should be displayed.
`asbr-summary`	Type 4 ASBR summary LSAs.
`external`	Type 5 external LSAs.
`network`	Type 2 network LSAs.
`router`	Type 1 router LSAs.
`summary`	Type 3 summary LSAs.
`nssa-external`	Type 7 NSSA external LSAs.
`opaque-link`	Type 9 LSAs which are not flooded beyond the local network.
`opaque-area`	Type 10 LSAs which are not flooded beyond the borders of their area.
`opaque-as`	Type 11 LSAs which are flooded throughout the AS.
`A.B.C.D`	Link state ID as an IP address.
`self-originate`	Display self-originated link states.
`adv-router`	Advertising router link states.
`A.B.C.D`	IPv4 address of advertising router.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: external and self-originate Parameters

This is sample output with the `external` and `self-originate` parameters.

```
#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)
```

```
 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Example: opaque-as and self-originate Parameters

This is sample output with the `opaque-as` and `self-originate` parameters.

```
#show ip ospf database opaque-as self-originate
 OSPF Router process 100 with ID (10.10.11.50)
 AS-Global Opaque-LSA
  LS age: 325
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external Opaque-LSA
  Link State ID: 11.10.9.23 (AS-external Opaque-Type/ID)
  Opaque Type: 11
  Opaque ID: 657687
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb018
 Length: 25
```

Example: adv-router Parameter

This is a sample output with the `adv-router` parameter.

```
#show ip ospf database nssa-external adv-router 10.10.11.50
 OSPF Router process 100 with ID (10.10.11.50)
 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 0.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xc9b6
  Length: 36
  Network Mask: /0
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 1
 NSSA: Forward Address: 0.0.0.0
OSPF Router process 100 with ID (10.10.11.50)
 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
```

```
   LS age: 78
   Options: 0x0 (*|-|-|-|-|-|-|-)
   LS Type: AS-NSSA-LSA
  Link State ID: 0.0.0.0 (External Network Number For NSSA)
```

Example: router and Link State ID Parameters

This is sample output with the `router` and link state ID parameters.

```
#show ip ospf database router 10.10.11.50
 OSPF Router process 100 with ID (10.10.11.50)
 Router Link States (Area 0.0.0.0)
  LS age: 878
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000004
  Checksum: 0xe39e
  Length: 36
Number of Links: 1
 Link connected to: Stub Network
 (Link ID) Network/subnet number: 10.10.10.0
 (Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
 TOS 0 Metric: 10
 Router Link States (Area 0.0.0.1)
  LS age: 877
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
 LS Seq Number: 80000003
```

Example: adv-router Parameter

This is sample output using the `adv-router` parameter for flood reduction.

```
#show ip ospf database summary adv-router 10.10.11.50

 OSPF Router process 100 with ID (10.10.11.50)
 Summary Link States (Area 0.0.0.0)
  LS age: 1(DoNotAge)
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10
Summary Link States (Area 0.0.0.1)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
```



```
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10

#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)

 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Database Detail Header Fields

Table 1-136 explains the fields for each database entry.

Table 1-136: ospf database detail header fields

Field	Description
LS age	Age of the LSA in seconds. “Do Not Age” is displayed if the DNA bit is set.
Options	LSA options as explained in Table 1-137.
Flags	ABR: Area border router ASBR: AS boundary router VL-endpoint: Endpoint of an active virtual link that is using the described area as a transit area Shortcut: shortcut ABR NSSA-Translator: NSSA border router with NSSA Translate or State enabled
LS Type	Type of LSA: Router-LSA Network-LSA Summary-LSA ASBR-summary-LSA AS-external-LSA AS-NSSA-LSA Link-Local Opaque-LSA Area-Local Opaque-LSA AS-external Opaque-LSA

Table 1-136: ospf database detail header fields

Field	Description
Link State ID	Identifier of the router described by the LSA.
Opaque Type	Opaque type used to identify the application type of the LSA: 9: link-local scope 10: area-local scope 11: LSA flooded throughout the AS
Opaque ID	Identifier used to differentiate LSAs of the same type.
Advertising Router	Identifier of the router that originated the LSA.
LS Seq Number	Sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
Checksum	Checksum of the entire LSA, except the LS age field.
Length	Length of the LSA
I LSA	Indication LSA: ASBR set the infinity metric to tell all routers in the backbone not to originate DNA LSAs.

OSPF LSA Option Bits

Table 1-137 explains the fields for each database entry.

Table 1-137: ospf LSA option bits output details

Bit	Description
DN	Used in MPLS-based L3 VPNs. When a route learned from a customer network via OSPF is advertised across a BGP/MPLS VPN using Multiprotocol BGP and advertised back to a customer network via OSPF, a loop can happen where the OSPF route is redistributed back to the VPN service provider network via BGP. The DN-bit prevents this type of routing loop. When an OSPF router receives a Type 3, 5, or 7 LSA with the DN-bit set, it foes use that LSA for OSPF route calculations.
O	Originating router supports Type 9, 10, and 11 Opaque LSAs.
DC	Originating router supports OSPF over Demand Circuits.
L	Whether the OSPF packet contains a Link-Local Signaling (LLS) data block. This bit is set only in Hello and database description packets.
N/P	The N-bit is used only in Hello packets when the originating router supports Type-7 NSSA-External-LSAs. Neighboring routers with mismatched N-bit will not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support NSSA capabilities. When the N-bit is set, the E-bit must be 0. The P-bit is used only in Type-7 NSSA-External-LSA headers. Due to this reason, the N- and P-bits share the same position in the options field. The P (Propagate) bit is set to inform an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
MC	Originating router supports multicast extensions to OSPF (MOSPF)

Table 1-137: ospf LSA option bits output details (Continued)

Bit	Description
E	Originating router accepts AS External LSAs. The bit is set in all AS External LSAs and in all LSAs originated in the backbone and non-stub areas; and is be set to 0 in all Hellos and LSAs originated within a stub area. Additionally, this bit is used in Hello packets to indicate the capability of a router interface to send and receive Type-5 AS-External-LSAs. Neighboring routers with mismatched E-bit do not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support the stub capabilities.
T	Originating router supports Multitopology OSPF (MT-OSPF.) Older OSPF specifications used this bit when the originating router support TOS-based routing. However, OSPF TOS-based routing was never deployed; therefore the T-bit was never used.

Type 1 Router LSAs (“router” Parameter)

Table 1-138 explains the fields for each database entry.

Table 1-138: router LSAs

Field	Description
Number of Links	Number of router links the LSA describes.
Link connected to	Description of the router link: another Router (point-to-point) a Transit Network Stub Network a Virtual Link
(Link ID)	Identifier of the router to which the link connects: Neighboring Router ID Designated Router address Network/subnet number Neighboring Router ID
(Link Data)	Extra information: Router Interface address Network Mask
Number of TOS metrics	Number of TOS (Type of Service) metrics for this link, not including the metric for TOS 0.
TOS 0 Metric	Cost of using this router link for TOS 0.

Type 2 Net Link States (“network” Parameter)

Table 1-139 explains the fields for each database entry.

Table 1-139: net LSAs

Field	Description
Network Mask	IP address mask for the network.
Attached Router	Identifiers of each router attached to the network.

Type 3 Summary LSAs (“summary” Parameter) and Type 4 ASBR Summary LSAs (“asbr-summary” Parameter)

Table 1-140 explains the fields for each database entry.

Table 1-140: summary and ASBR summary link states

Field	Description
Network Mask	For Type 3 LSAs, the destination network's IP address mask. Not meaningful for Type 4 link state advertisements.
TOS: 0 Metric	Cost of using this router link for TOS 0.

Type 5 AS External LSAs (“external” Parameter)

Table 1-141 explains the fields for each database entry.

Table 1-141: external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
TOS	Always zero.
Metric	The cost of this route.
Forward Address	Data traffic for the advertised destination is forwarded to this address.
External Route Tag	Custom field attached to each external route whose use is defined by the application.

Type 7 NSSA External Link States (“nssa-external” Parameter)

Table 1-142 explains the fields for each database entry.

Table 1-142: NSSA external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
Metric	The cost of this route.
NSSA: Forward Address	Data traffic for the advertised destination is forwarded to this address.
External Route Tag	Custom field attached to each external route whose use is defined by the application.

show ip ospf igp-shortcut-lsp

Use this command to show the IGP shortcut LSP used by OSPF.

Command Syntax

```
show ip ospf igp-shortcut-lsp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf igp-shortcut-lsp
 Tunnel-endpoint     Tunnel-id     Tunnel-metric
 8.8.8.8             101           2              active
```

Table 1-143 explains the fields in the output.

Table 1-143: show ip ospf igp-shortcut-lsp output details

Field	Description
Tunnel-endpoint	Tunnel endpoint address of ospf.
Tunnel-id	Tunnel address (destination port) for the session.
Tunnel-metric	Number of tunnel-metric.
active/inactive	Whether the tunnel is active or inactive.

show ip ospf igp-shortcut-route

Use this command to show the IGP shortcut route calculated by OSPF.

Command Syntax

```
show ip ospf (<0-65535>|) igp-shortcut-route
```

Parameters

`<0-65535>`	ID of the router process.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf igp-shortcut-route
OSPF process 0:
8.8.8.8/32 [2] tunnel-id: 101, 8.8.8.8
15.15.15.15/32 [0] tunnel-id: 101, 8.8.8.8
20.20.15.0/24 [0] tunnel-id: 101, 8.8.8.8
```

Table 1-144 explains the fields in the output.

Table 1-144: show ip igp-shortcut-route output details

Field	Description
OSPF process	OSPF process identifier.
Destination	IP address of the destination port.
Metric	Number of tunnel metric.
Tunnel-ID	Tunnel address (destination port) for the session.
Tunnel-End-Point	Tunnel endpoint address of ospf.

show ip ospf interface

Use this command to display interface information for OSPF.

Command Syntax

```
show ip ospf interface (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf interface
eth1 is up, line protocol is up
 Internet Address 10.100.10.72/24, Area 0.0.0.0, MTU 1500
    Router ID 100.100.100.72, Network Type BROADCAST, Cost: 10, TE Metric 0
    Transmit Delay is 1 sec, State DR, Priority 1
    LDP-OSPF Sync configured
    Holddown timer : 50 seconds, Remaining time =  30seconds
    Designated Router (ID) 100.100.100.72, Interface Address 10.100.10.72
    Backup Designated Router (ID) 10.100.12.57, Interface Address 10.100.10.105
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:05
    Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
    Hello received 19 sent 106, DD received 4 sent 3
    LS-Req received 1 sent 1, LS-Upd received 3 sent 3
    LS-Ack received 2 sent 3, Discarded 0
```

OSPF Interface Fields

Table 1-145 explains the fields for each interface entry.

Table 1-145: OSPF interface output details

Field	Description
Internet address	IP address and subnet mask of the interface.
Area	OSPF area to which the interface belongs.
MTU	Maximum Transmission Unit (MTU) of the interface.
Transmit Delay	Transmit delay of the interface.

Table 1-145: OSPF interface output details

Field	Description
Priority	OSPF priority of the interface used for election of Designated Router (DR) and Backup Designated Router (BDR).
Hello	OSPF hello-interval.
Dead	OSPF dead-interval.
Wait	Hello wait-interval.
Retransmit	The period, in seconds, for which the router waits between retransmissions of OSPF packets that have not been acknowledged.
Hello due in	Time period for which router expects to receive hello packet.
Neighbor Count	OSPF neighbor count.
Adjacent neighbor	OSPF adjacent neighbor count.
Crypt Sequence Number	Used for authentication.
Hello received	Number of Hello packets and DD packets sent and received.
LS-Req	Number of LSA requests and LSA updates sent and received.
LS-Ack	Number of LSA acknowledgments sent and received number of LSA acknowledgment discards.

Example: DoNotAge

The following is sample output of this command when DoNotAge is enabled:

```
#show ip ospf interface eth1
eth1 is up, line protocol is up
 Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
 Process ID 0, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State Waiting, Priority 1, TE Metric 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Neighbor Count is 0, Adjacent neighbor count is 0
 Crypt Sequence Number is 1106347721
 Hello received 0 sent 1, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
 Reduce LSA flooding
```

Example: Hello Suppression

The following is sample output of this command when Hello-Suppression is enabled:

```
#sh ip os interface
p7p1 is up, line protocol is up
  Internet Address 14.1.1.2/24, Area 0.0.0.0, MTU 1500
```

```
  Process ID 1, VRF (default), Router ID 2.2.2.2, Network Type POINTOMULTIPOINT, Cost:
1
  Reduce LSA flooding.
  Transmit Delay is 1 sec,  State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 1 neighbor(s)
  Hello received 5 sent 8, DD received 8 sent 6
  LS-Req received 2 sent 2, LS-Upd received 8 sent 9
  LS-Ack received 6 sent 6, Discarded 0
  No authentication
```

show ip ospf multi-area-adjacencies

Use this command to display multi-area adjacency information for OSPF.

Command Syntax

```
show ip ospf (<0-65535>|) multi-area-adjacencies
```

Parameters

`<0-65535>`	The ID of the router process for which information should be displayed.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command:

```
#show ip ospf 1 multi-area-adjacencies

Multi-area-adjacency on interface eth1 to neighbor 20.20.20.10
Internet Address 20.20.20.11/24, Area 0.0.0.1, MTU 1500
Process ID 1, Router ID 10.10.10.10, Network Type POINTOPOINT, Cost: 10
Transmit Delay is 1 sec, State Point-To-Point
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 1229928206
Hello received 0 sent 513, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

Table 1-146 explains the fields for each adjacency entry.

Table 1-146: show ip ospf multi-area-adjacencies output details

Field	Description
Multi-area-adjacency	Specifies the interface name and the router ID to which it is connected.
Internet Address	As Stated
Area	As Stated
MTU	Maximum Transmission Unit in bytes.
Process ID	The Process Identifier.
Router ID	As Stated
Network Type	In multi-area adjacencies, this is a point-to-point network with the neighbor.

Table 1-146: show ip ospf multi-area-adjacencies output details (Continued)

Field	Description
Cost	A reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is reference bandwidth divided by interface bandwidth.
Transmit Delay	A stated
State	As stated
Timer intervals configured	Hello timer = 10, Dead timer = 40, Wait timer = 40, Retransmit timer = 5
Hello due in	Countdown timer for a Hello message from the neighbor.
Neighbor Count	The number of neighbor.
Adjacent neighbor count	The number of neighbors participating in adjacencies.
Crypt Sequence Number	The 32-bit cryptographic sequence number appended on each OSPF protocol packet.
Hello received, sent	Hello packets sent and received.
DD received, sent	Database Description packets sent and received.
LS-Req received, sent	Link State Request packets sent and received.
LS-Upd received, sent	Link State Update packets sent and received.
LS-Ack received, sent, discarded	Link State Acknowledgement packets sent, received, or discarded.

show ip ospf neighbor

Use this command to display information about OSPF neighbors.

Command Syntax

```
show ip ospf (<0-65535>|) neighbor
show ip ospf (<0-65535>|) neighbor all
show ip ospf (<0-65535>|) neighbor interface A.B.C.D
show ip ospf (<0-65535>|) neighbor A.B.C.D
show ip ospf (<0-65535>|) neighbor A.B.C.D detail
show ip ospf (<0-65535>|) neighbor detail
show ip ospf (<0-65535>|) neighbor detail all
```

Parameters

`<0-65535>`	The ID of the router process
`all`	Include downstatus neighbor
`A.B.C.D`	IPv4 address
`detail`	Details of neighbors

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State       Dead Time   Address      Interface    Instance ID
1.1.1.1           1   Full/ -     inactive    14.1.1.1     p7p1                0
3.3.3.3           1   Full/ -     00:01:41    15.1.1.2     p8p1                0
3.3.3.3           1   Full/ -     inactive    15.1.1.2     VLINK0
```

OSPF Neighbor Fields

Table 1-147 explains the fields for each neighbor entry.

Table 1-147: OSPF neighbor output details

Field	Description
OSPF process	OSPF process identifier.
Neighbor ID	OSPF router identifier of the neighbor.

Table 1-147: OSPF neighbor output details

Field	Description
Pri	OSPF priority of the neighbor.
State	State of the OSPF neighbor: DependUpon: dummy state Down: no OSPF neighbors detected at this instant Attempt: in an NBMA environment, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval Init: hello packet received, but the receiving router's ID was not included in the hello packet 2-Way: bi-directional communication established between two routers ExStart: master and slave roles determined Exchange: database description packets (DBD) sent Loading: exchange of LSRs (link state request) and LSUs (link state update) packets Full: routers fully adjacent with each other.
Dead Time	If a new Hello is not received within this duration, the neighbor is declared dead.
Address	IP address of neighbor's interface attached to the network.
Interface	The interface attached to the network on which the neighbor is located.
Instance ID	Instance identifier for the session.

Example: Detail Parameter

This is sample output from the command when the `detail` parameter is specified:

```
#show ip ospf neighbor detail
 Neighbor 10.10.10.50, interface address 10.10.10.50
 In the area 0.0.0.0 via interface eth0
 Neighbor priority is 1, State is Full, 5 state changes
 DR is 10.10.10.50, BDR is 10.10.10.10
 Options is 0x42 (*|O|-|-|-|-|E|-)
 Dead timer due in 00:00:38
 Neighbor is up for 00:53:07
 Database Summary List 0
 Link State Request List 0
 Link State Retransmission List 0
 Crypt Sequence Number is 0
 Thread Inactivity Timer on
 Thread Database Description Retransmission off
```

OSPF Neighbor Detail Fields

Table 1-148 explains the fields for each neighbor detail entry.

Table 1-148: OSPF neighbor output detail

Field	Description
Neighbor	OSPF router identifier of the neighbor.
interface address	IP address of the neighbor interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	OSPF priority of the neighbor.
State	OSPF state as explained in Table 1-147.
state changes	Number of state changes since the neighbor was created.
Hello is suppressed	Hello suppression is enabled.
Poll interval	Poll timer value.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	LSA options as explained in Table 1-137.
LLS Options	LSDB Resynchronization (LR) Restart Signal (RS-bit) Whether link-local signalling (LLS) and out-of-band (OOB) link-state database resynchronization are performed for nonstop forwarding (NSF).
OOB-Resync in progress (receiver)/last OOB-Resync	Last successful OOB resynchronization with the NSF-capable neighbor. The router waits before taking a neighbor adjacency down if the OOB resynchronization has not taken place since the time a restart signal (Hello packet with RS-bit set) was received from the neighbor.
Dead timer due in	Expected time before declaring the neighbor dead.
Poll due in	Poll timer thread.
Neighbor is up for	Time since the neighbor went into the two-way state.
Database Summary List	Number of LSAs in the neighbor’s database.
Link State Request List	Number of LSAs that need to be received from this neighbor to synchronize the neighbors' topological databases.
Link State Retransmission List	Number of advertisements flooded out an adjacency. To ensure flooding is reliable, advertisements are retransmitted until they are acknowledged.
Crypt Sequence Number is	MD5 cryptographic sequence number.
Thread Inactivity Timer	Off if hello suppression is enabled, on otherwise.
Thread Database Description Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Link State Request Retransmission	Off if hello suppression is enabled, on otherwise.

Table 1-148: OSPF neighbor output detail (Continued)

Field	Description
Thread Link State Update Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Poll Timer	Whether the poll timer thread is on.
Bidirectional Forwarding Detection is enabled	Status of BFD, enabled or disabled.

Example: Hello-Suppression Option

This is sample output from the command when the `detail` parameter is specified and Hello-Suppression is enabled:

```
#sh ip os neighbor detail
 Neighbor 1.1.1.1, interface address 14.1.1.1
    In the area 0.0.0.0 via interface p7p1
    Neighbor priority is 1, State is Full, 5 state changes
    Hello is suppressed
    DR is 0.0.0.0, BDR is 0.0.0.0
    Options is 0x62 (-|O|DC|-|-|-|E|-)
    Dead timer due in inactive
    Neighbor is up for 00:05:03
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer off
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission off
```

show ip ospf route

Use this command to display the OSPF routing table.

Command Syntax

```
show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary |)
show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary | fast-reroute |)
```

Parameters

`<0-65535>`	Router process identifier.
`A.B.C.D`	Single route.
`A.B.C.D/M`	Single exact match route.
`summary`	Route counts.
`fast-reroute`	Fast-reroute routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf route
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 80.0.0.0/24 [1] is directly connected, eth4, Area 0.0.0.15
```

Header

Each entry in this table has a code preceding it indicating the source of the routing entry.

Table 1-149 explains the fields of route codes.

Table 1-149: route codes

Code	Meaning	Description
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from routing protocols.
O	OSPF	Modifiers: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
D	discard	An ABR or ASBR performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.

Route Entry Fields

Table 1-150 shows the route entry fields.

Table 1-150: route entry output details

Field	Description
Codes	As explained in Table 1-149.
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Area	OSPF area identifier

Example: Process Identifier

The following is a sample output with the process identifier parameter.

```
#show ip ospf 10 route
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
```

show ip ospf valid

Use this command to display information about opaque LSAs.

Command Syntax

```
show ip ospf (<0-65535>|) opaque-link valid
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.
`opaque-link`	Displays information about the opaque link-local LSAs.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf 1 opaque-link valid
```

show ip ospf virtual-links

Use this command to display virtual link information.

Command Syntax

```
show ip ospf (<0-65535>|) virtual-links (brief|)
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.
`brief`	Display summary of OSPF virtual-links.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down.

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
 Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in inactive
 Adjacency state Down
```

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down when flood reduction is enabled

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
 Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in inactive
 Adjacency state Down
```

```
    DoNotAge LSA Allowed
```

If Hello-Suppression is enabled

```
    M1#sh ip os virtual-links
    Virtual Link VLINK0 to router 3.3.3.3 is up
      Transit area 0.0.0.1 via interface p8p1
      Hello suppression enabled
      DoNotAge LSA allowed
      Local address 15.1.1.1/32
      Remote address 15.1.1.2/32
      Transmit Delay is 1 sec, State Point-To-Point,
      Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        Hello due in inactive
      No authentication
        Adjacency state Full
    M1#
```

Table 1-151 explains the fields for each virtual-links entry.

Table 1-151: show ip ospf virtual-links output details

Field	Description
Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IP address and subnet mask.
Remote address	The remote IP address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 0 to 65535. The default is 1. The state is point-to-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ip protocols

Use this command to display OSPF process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols ospf
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This is an example of the output from the `show ip protocols` command:

```
#show ip protocols
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
 Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
 192.30.30.0/24
 192.40.40.0/24
  Routing Information Sources:
 GatewayDistanceLast Update
  Distance: (default is 110)
 AddressMaskDistance List
```

Table 1-152 explains the fields for each ip protocol entry.

Table 1-152: show ip protocols output details

Field	Description
Routing Protocol is "ospf 200"	Specifies the routing protocol used.
Invalid after 0 seconds	Specifies the value of the invalid parameter.
Hold down 0	Specifies the current value of the hold-down parameter.
Flushed after 0	Specifies the time in seconds after which the individual routing information will be thrown (flushed) out.
Outgoing update	Specifies whether the outgoing filtering list has been set.

Table 1-152: show ip protocols output details

Field	Description
Incoming update	Specifies whether the incoming filtering list has been set.
Redistributing	Lists the protocol that is being redistributed.
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the IP Infusion software is using to build its routing table.

show ip route fast-reroute

Use this command to display routes with alternate next hops.

Command Syntax

```
show ip route fast-reroute
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip route fast-reroute
```

shutdown

Use the this command to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away.

Use the no parameter of this command.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#shutdown

#configure terminal
(config)#router ospf 100
(config-router)#no shutdown
```

snmp restart ospf

Use this command restart SNMP in OSPF

Command Syntax

```
snmp restart ospf
```

Parameter

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart ospf
```

summary-address

Use this command to summarize or suppress external routes with the specified address range.

Use the no option with this command to disable summary address.

An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Command Syntax

```
summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag <0-4294967295>|)
no summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag (<0-
  4294967295>|))
```

Parameters

`A.B.C.D/M`	The range of addresses given as IPv4 starting address and a mask.
`A.B.C.D`	IP summary prefix e.g. i.i.i.i
`A.B.C.D`	IP summary prefix mask e.g. m.m.m.m
`not-advertise`	Suppress routes that match the range.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps.
`<0-4294967295>`	Set a tag value.

Default

By default, tag value is 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#summary-address 172.16.0.0/16 tag 3
```

timers lsa arrival

This command sets the minimum interval to accept the same link-state advertisement (LSA) from OSPF neighbors.

Use the no form of this command to restore the default value.

Command Syntax

```
timers lsa arrival <0-600000>
no timers lsa arrival
```

Parameters

<0-600000>	The minimum delay in milliseconds between accepting the same LSA from neighbors.

Default

By default, Minimum LSA Arrival timer is 1 sec.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers lsa arrival 5000
```

timers spf exp

Use this command to set the Shortest-Path First (SPF) best-path schedule minimum and maximum delay between receiving a change to SPF calculation in milliseconds.

Use no parameter of this command to unset the SPF best-path schedule.

Command Syntax

```
timers spf exp <0-2147483647> <0-2147483647>
no timers spf exp
```

Parameters

<0-2147483647>	The minimum delay in milliseconds between receiving a change to SPF calculation.
<0-2147483647>	The maximum delay in milliseconds between receiving a change to SPF calculation.

Default

Default minimum delay: 500 milliseconds

Default maximum delay: 50000 milliseconds (50 seconds)

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers spf exp 300 300
```

timers throttle lsa

This command sets the rate-limiting intervals for OSPF link-state advertisement (LSA) generation.

Use the no form of this command to restore the default values.

Command Syntax

```
timers throttle lsa all <0-600000> <1-600000> <1-600000>
no timers throttle lsa all
```

Parameters

<0-600000>	Start interval: The minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF topology change. The generation of the next LSA is not before the start interval.
<0-600000>	Hold interval: The hold time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation.
<0-600000>	Maximum interval: The maximum wait time in milliseconds between generation of the same LSA.

Defaults

Default start interval: 0 milliseconds

Default hold interval: 5000 milliseconds

Default maximum interval: 5000 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers throttle lsa all 200 10000 45000
```

CHAPTER 2 OSPFv2 Graceful Restart Commands

This chapter describes the OSPFv2 graceful restart commands.

capability restart

Use this command to enable OSPF graceful restart or restart signaling. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the no parameter with this command to disable the features.

Command Syntax

```
capability restart graceful
no capability restart graceful
```

Parameters

None

Default

By default, OSPF graceful restart or restart signaling is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability restart graceful

(config)#router ospf 100
(config-router)#no capability restart graceful
```

debug ip ospf graceful-restart

Use this command to specify debugging option for OSPF graceful restart.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ip ospf graceful-restart (detail|terse|)
no debug ip ospf graceful-restart (detail|terse|)
```

Parameters

detail	Debug OSPF graceful restart detail information
terse	Debug OSPF graceful restart summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf graceful-restart detail
```

ospf restart grace-period

Use this command to set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the no parameter with this command to revert to the default.

Command Syntax

```
ospf restart grace-period <1-1800>
no ospf restart grace-period
```

Parameters

<1-1800>	Gace period in seconds.

Default

The default grace period for restarting the OSPF router is 120 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ospf restart grace-period 250
```

ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the no parameter with this command to revert to default.

Command Syntax

```
ospf restart helper {max-grace-period <1-1800>}
ospf restart helper never (router-id A.B.C.D|)
no ospf restart helper (never router-id (A.B.C.D | all) | max-grace-period|)
```

Parameters

<1-1800>	Help only if received grace-period is less than this value.
A.B.C.D	Router ID of neighbor to never to act as helper.
never	Prevent the neighbor from entering helper mode.
all	All neighbors to never to act as helper.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#no ospf restart helper never router-id all
```

restart ospf graceful

Use this command to restart OSPF gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax

```
restart ospf graceful (grace-period <1-1800>|)
```

Parameters

<1-1800>	Grace period in seconds.

Default

No default value is specified

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart ospf graceful grace-period 200
```

CHAPTER 3 OSPFv3 Commands

This chapter provides an alphabetized reference for each of the OSPFv3 commands. It includes the following commands:

- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- ipv6 te-metric
- max-concurrent-dd
- passive-interface
- redistribute
- router-id
- router ipv6 ospf
- show debugging ipv6 ospf
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 route fast-reroute
- show ipv6 ospfv3 topology
- show ipv6 ospf virtual-links
- show ipv6 vrf
- snmp restart ospf6
- summary-address

abr-type

Use this command to set an OSPFv3 Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax

```
abr-type (cisco|ibm|standard)
no abr-type (cisco|ibm|standard|)
```

Parameters

`cisco`	Specify an alternative ABR using Cisco implementation. This is the default ABR type.
`ibm`	Specify an alternative ABR using IBM implementation.
`standard`	Specify a standard ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#abr-type standard
```

address-family ipv4 unicast

Use this command to enter address family mode where you can configure IPv4 unicast addresses for OSPFv3, including:

- Summarizing intra-area IPv4 routes (area range command)
- Create a default external route (default-information originate command)
- Redistributing IPv4 routes (redistribute command)
- Summarizing IPv4 external routes (summary-address command)

RFC 5838 defines the range of instance IDs below to use for each address family in OSPFv3.

TABLE 2.

Instance ID#	Address Family
0 - 31	IPv6 unicast
64 - 95	IPv4 unicast

Multiple router processes can configured per interface, but only one instance per router per interface can be configured. Each instance ID creates a separate OSPFv3 instance with its own neighbor adjacencies, link state database, and SPF computation. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the *same* interface is not supported.

To leave the address family mode and return to the configure mode, use the `exit-address-family` command.

Use the no form of this command to remove the address-family configuration.

Command Syntax

```
address-family ipv4 unicast
no address-family
```

Parameters

None

Default

By default, OSPFv3 supports only IPv6 unicast traffic.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#address-family ipv4 unicast
```

area default-cost

Use this command to specify the cost for default summary route sent into a stub area. If an area is configured as a stub, the OSPFv3 router originates one type-3 inter-area-prefix-LSA into the stub area. This command changes the metric for this LSA.

Use the no parameter with this command to remove the assigned default cost.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) default-cost (<0-16777215>)
no area (A.B.C.D|<0-4294967295>) default-cost (<0-16777215>|)
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
<0-16777215>	The advertised cost for the default summary route used for a stub or NSSA area.

Default

By default, advertised cost for the default summary route is 1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 default-cost 10
```

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the no form of this command to make an area a normal area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) nssa
area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)|stability-
  interval <0-2147483647>|no-redistribution|default-information-originate (metric
  <0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-2>|metric-type
  <1-2> metric <0-16777214>|)|no-summary}
no area (A.B.C.D|<0-4294967295>) nssa
no area (A.B.C.D|<0-4294967295>) nssa {translator-role|stability-interval|no-
  redistribution|default-information-originate|no-summary}
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
translator-role	NSSA-ABR translator role:
candidate	Translate NSSA-LSA to Type-5 LSA if router is elected.
always	Always translate NSSA-LSA to Type-5 LSA.
stability-interval	Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.
<0-2147483647>	Stability interval in seconds.
no-redistribution	Do not redistribute into the NSSA.
default-information-originate	Originate Type-7 default LSA into the NSSA.
metric	Specify metric for default routes.
<0-16777214>	Specify metric value.
metric-type	Specify metric type (see RFC 3101).

<1-2>	Specify metric type: 1: Type 1 external route 2: Type 2 external route
no-summary	Do not inject inter-area routes into the NSSA.
translate-candidate	Translate NSSA-LSA to Type-5 LSA if router is elected.
translate-always	Always translate NSSA-LSA to Type-5 LSA.

Default

By default, the nssa option value is candidate.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ipv6 ospf
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```

area range

Use this command to configure the OSPF address range. This command summarizes intra-area routes for an area. The single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the no parameter with this command to remove the assigned area range.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) range X:X::X:X/M
area (A.B.C.D|<0-4294967295>) range A.B.C.D/M
area (A.B.C.D|<0-4294967295>) range X:X::X:X/M (advertise|not-advertise)
area (A.B.C.D|<0-4294967295>) range A.B.C.D/M (advertise|not-advertise)
no area (A.B.C.D|<0-4294967295>) range X:X::X:X/M
no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
X:X::X:X/M	The area IPv6 range prefix and length.
A.B.C.D/M	The area IPv4 range prefix and length.
advertise	Advertises this range.
not-advertise	Does not advertise this range.

Default

No default value is specified

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 range 2000::/3

#configure terminal
(config)#router ipv6 ospf 10
(config-router)#router-id 10.10.10.10
(config-router)#address-family ipv4 unicast
(config-router-af)#area 1 range 10.0.0.0/8
```

```
(config-router-af)#exit-address-family
```

area stub

Use this command to define an area as a stub area on all routers. There are two stub area router configuration commands: the `stub` and commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area` command.

Use the `no` form of this command to make an area a normal area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) stub
area (A.B.C.D|<0-4294967295>) stub no-summary
no area (A.B.C.D|<0-4294967295>) stub
no area (A.B.C.D|<0-4294967295>) stub no-summary
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`no-summary`	Stops an ABR from sending summary link advertisements into the stub area.

Default

No stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 stub no-summary
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other nonbackbone areas.

Use the no parameter with this command to remove the virtual link.

In OSPFv3, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the `hello-interval` to be the same for all routers attached to a common network. If the `hello-interval` is short, the router detects topological changes faster, but more routing traffic follows.

The `retransmit-interval` is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The `transmit-delay` is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet are increased by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval|hello-
  interval|retransmit-interval|transmit-delay) <1-65535>
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id (<0-31>|<64-95>)
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval|hello-
  interval|retransmit-interval|transmit-delay)
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id
```

Parameters

`A.B.C.D`	OSPF Area ID in IP64 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D`	Specify router ID associated with a virtual link neighbor.
`dead-interval`	The interval in seconds during which no packets are received and after which the router acknowledges a neighboring router as off-line.
`hello-interval`	The interval in seconds the router waits before it sends a hello packet.
`retransmit-interval`	The interval in seconds the router waits before it retransmits a packet.
`transmit-delay`	The interval in seconds the router waits before it transmits a packet.
`<1-65535>`	The timer interval.
`instance-id`	The OSPFv3 instance.
`<0-31>`	Interface instance ID for IPv6 unicast

`<64-95>`	Interface instance ID for IPv4 unicast.
`fall-over bfd`	Fall-over Bidirectional Forwarding Detection (BFD).

Default

Default hello interval:10 seconds.

Default dead interval:40 seconds.

Default retransmit interval: 5 seconds.

Default transmit delay: 1 second

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
(config-router)#area 1 virtual-link 10.10.11.50 instance-id 1
(config-router)#area 1 virtual-link 10.10.11.50 fall-over bfd
```

auto-cost reference bandwidth

Use this command to control how OSPFv3 calculates default metrics for the interface.

By default, OSPFv3 calculates the OSPFv3 metric for an interface by dividing the reference bandwidth by the interface bandwidth. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Use the no form of this command to assign cost based only on the interface bandwidth.

Command Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameters

<1-4294967>	The reference bandwidth in Mbps per second.

Default

By default, reference bandwidth is 100Mbps

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example changes the reference bandwidth to 1Gbps to change the Fast Ethernet interface cost from 1 to 10.

```
#configure terminal
(config)#router ipv6 ospf 1
(config-router)#auto-cost reference-bandwidth 1000

(config)#router ipv6 ospf 1
(config-router)#no auto-cost reference-bandwidth
```

capability cspf

Use this command to enable the CSPF (Constrained Shortest Path First) feature for an OSPFv2 or OSPFv3 instance.

Use the no parameter with this command to disable CSPF functionality for the OSPFv2 or OSPFv3 instance.

Command Syntax

```
capability cspf
no capability cspf
```

Parameters

None

Default

By default, capability cspf is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#no capability cspf
```

clear ipv6 ospf process

Use this command to clear and restart all OSPFv3 routing processes or a given OSPFv3 routing process.

Command Syntax

```
clear ipv6 ospf (WORD|) process
```

Parameters

WORD	OSPFv3 process tag.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 ospf Tag1 process
```

debug ipv6 ospf

Use this command to specify all debugging options for OSPFv3.

Use the no form of this command to disable the options.

Command Syntax

```
debug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|)

no debug ipv6 ospf
  (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|)
undebug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|rib|route)
no debug all ipv6 ospf
undebug all ipv6 ospf
no debug all
undebug all
```

Parameters

`all`	Enables all debugging information.
`bfd`	Debug OSPFv3 Bidirectional Forwarding Detection. (see debug ipv6 ospf bfd)
`events`	Debug OSPFv3 events (see debug ipv6 ospf events).
`ifsm`	Debug OSPFv3 Interface State Machines (see debug ipv6 ospf ifsm).
`lsa`	Debug OSPFv3 Link State Advertisements (see debug ipv6 ospf lsa).
`nfsm`	Debug OSPFv3 Neighbor State Machines (see debug ipv6 ospf nfsm).
`nsm`	Debug OSPFv3 NSM information (see debug ipv6 ospf nsm).
`packet`	Debug OSPFv3 packets (see debug ipv6 ospf packet).
`retransmission`	Debug OSPFv3 retransmission information. (see debug ipv6 ospf retransmission)
`rib`	Debug OSPFv3 Routing Information Base.(see debug ipv6 ospf rib)
`route`	Debug OSPFv3 route information (see debug ipv6 ospf route).

Command Mode

Privileged Exec and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf all
```

debug ipv6 ospf bfd

Use this command to specify the debugging options for OSPFv3 Bidirectional Forwarding Detection

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf bfd
no debug ipv6 ospf bfd
undebug ipv6 ospf bfd
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf bfd
```

debug ipv6 ospf events

Use this command to display debug information related to OSPF internal events. Use this command without parameters to turn on all the options.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
no debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
undebug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
```

Parameters

`abr`	Debug ABR events
`asbr`	Debug ASBR events
`os`	Debug OS interaction events
`router`	Debug other router events
`vlink`	Debug virtual link events
`nssa`	Debug NSSA events

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ipv6 ospf events abr
#debug ipv6 ospf events asbr
```

debug ipv6 ospf ifsm

Use this command to specify debugging options for OSPFv3 Interface Finite State Machine (IFSM) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf ifsm ({events|status|timers}|)
no debug ipv6 ospf ifsm ({events|status|timers}|)
undebug ipv6 ospf ifsm ({events|status|timers}|)
```

Parameters

events	Debug IFSM event information.
status	Debug IFSM status information.
timers	Debug IFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf ifsm status
```

debug ipv6 ospf lsa

Use this command to specify the debugging options for OSPFv3 Link State Advertisements (LSAs).

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
no debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
undebug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
```

Parameters

`generate`	Debug LSA generation.
`flooding`	Debug LSA flooding.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf lsa
```

debug ipv6 ospf nfsm

Use this command to specify debugging options for OSPFv3 Neighbor Finite State Machines (NFSMs).

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf nfsm {(events|status|timers)|}
no debug ipv6 ospf nfsm {(events|status|timers)|}
undebug ipv6 ospf nfsm {(events|status|timers)|}
```

Parameters

events	Debug NFSM event information.
status	Debug NFSM status information.
timers	Debug NFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf nfsm events
#no debug ipv6 ospf nfsm timers
```

debug ipv6 ospf nsm

Use this command to specify the debugging options for OSPFv3 NSM information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf nsm {(interface|redistribute)|}
no debug ipv6 ospf nsm {(interface|redistribute)|}
undebug ipv6 ospf nsm {(interface|redistribute)|}
```

Parameters

`redistribute`	Debug redistribute.
`interface`	Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf nsm interface
```

debug ipv6 ospf packet

Use this command to specify the packet debugging options for OSPFv3 information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)


no debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|
  detail}|)
undebug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPFv3 hello.
`dd`	Debug OSPFv3 database description.
`ls-request`	Debug OSPFv3 link state request.
`ls-update`	Debug OSPFv3 link state update.
`ls-ack`	Debug OSPFv3 link state acknowledgment.
`send`	Debug packets sent
`recv`	Debug packets received.
`detail`	Debug detail information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf packet ls-request
```

debug ipv6 ospf retransmission

Use this command to specify the debugging options for OSPFv3 retransmission information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf retransmission
no debug ipv6 ospf retransmission
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf retransmission
```

debug ipv6 ospf rib

Use this command to specify the debugging options for OSPFv3 RIB information.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf rib {(interface|redistribute)|}

no debug ipv6 ospf rib {(interface|redistribute)|}
undebug ipv6 ospf rib {(interface|redistribute)|}
```

Parameters

redistribute	Debug redistribute.
interface	Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf rib interface
```

debug ipv6 ospf route

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf route {(ase|ia|install|spf)|}
no debug ipv6 ospf route {(ase|ia|install|spf)|}
undebug ipv6 ospf route {(ase|ia|install|spf)|}
```

Parameters

`ase`	Debug external route calculations.
`ia`	Debug inter-area route calculations.
`install`	Debug the route installation.
`spf`	Debug the SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ipv6 ospf route
#debug ipv6 ospf route ia
```

default-information originate

Use this command to create a default external route into an OSPF routing domain.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
default-information originate
default-information originate {metric <0-16777214>|metric-type (1|2)|route-map
  WORD|always}
no default-information originate
no default-information originate {metric|metric-type|route-map|always}
```

Parameters

`always`	Used to advertise the default route regardless of whether there is a default route.
`metric`	Sets the OSPF metric used in creating the default route.
`<0-16777214>`	Sets the OSPF metric used in creating the default route. The value used is specific to the protocol.
`metric-type`	The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).
`1`	Sets OSPF External Type 1 metric.
`2`	Sets OSPF External Type 2 metric (default).
`route-map`	Route map.
`WORD`	Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 sets OSPF External Type 2 metric

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-information originate always metric 23 metric-type 2
route-map myinfo

(config)#router ipv6 ospf
(config-router)#no default-information originate metric metric-type route-map
```

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the no parameter with this command to return to the default state.

Command Syntax

```
default-metric <1-16777214>
no default-metric
no default-metric <1-16777214>
```

Parameter

<1-16777214>	Default metric value.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-metric 100
```

distance

Use this command to define OSPFv3 route administrative distances based on route type. This command sets the distance for an entire group of routes rather than a specific route that passes an access list.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 254 means that the routing information source cannot be trusted and should be ignored.

Use the no form of this command to restore the default value.

Command Syntax

```
distance <1-254>
distance ospfv3 {intra-area <1-254>|inter-area <1-254>|external <1-254>}
no distance (<1-254>|)
no distance ospfv3 {intra-area |inter-area |external}
```

Parameters

`<1-254>`	Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.
`intra-area`	Routes within an area.
`<1-254>`	Distance for all routes within an area
`inter-area`	Routes from one area to another area.
`<1-254>`	Distance for all routes from one area to another area.
`external`	Routes from other routing domains learned by redistribution.
`<1-254>`	Distance for routes from other routing domains learned by redistribution.

Default

By default, distance value for each type of route is 110

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#distance ospfv3 inter-area 20 intra-area 10 external 40
```

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the no parameter with this command to disable this function.

Command Syntax

```
distribute-list WORD out ((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|)))
distribute-list WORD in
no distribute-list WORD out ((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|)))
no distribute-list WORD in
```

Parameters

WORD	Specify the name of the access list.
in	Filter incoming routing updates.
out	Filter outgoing routing updates.
kernel	Specify kernel routes.
connected	Specify connected routes.
static	Specify static routes.
rip	Specify RIP routes.
bgp	Specify BGP routes.
isis	Specify IS-IS routes.
ospf	Specify OSPF routes.
WORD	Specify the OSPF process tag. If not specified, redistribute OSPF process with tag "null".
<1-65535>	Specify OSPF process ID <1-65535>. If not specified, redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list list1 (network 172.10.0.0).

```
#configure terminal
(config)#access-list list1 permit 172.10.0.0/16
```

```
(config)#router ipv6 ospf 100
(config-router)#distribute-list list1 out bgp
(config-router)#redistribute bgp
```

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv3.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor if the LSA instance in the summary list is the same as or less recent than the LSA in the database description packet received from the neighbor.

Use the no form of the command to disable database summary list optimization.

Command Syntax

```
enable db-summary-opt
no enable db-summary-opt
```

Parameters

None

Default

By default, db summary opt is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```

exit-address-family

Use this command to exit address-family mode and return to router mode.

Command Syntax

```
exit-address-family
```

Parameters

None

Default

By default, exit address family is disabled

Command Mode

Router address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config) # router ipv6 ospf 10
(config-router) # router-id 10.10.10.10
(config-router) # address-family ipv4 unicast
(config-router-af) # area 1 range 10.0.0.0/8
(config-router-af) # exit-address-family
```

ipv6 ospf cost

Use this command to specify the link-cost described in LSAs.

The cost (or metric) of an interface in OSPF indicates the overhead required to send packets across a certain interface. The value is taken to describe Link State information, and used for route calculation.

Use the no parameter with this command to reset the cost to default.

Command Syntax

```
ipv6 ospf cost <1-65535>
ipv6 ospf cost <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf cost
no ipv6 ospf cost instance-id (<0-31>|<64-95>)
```

Parameters

cost	Specify the link-state metric.
<1-65535>	Specify the link-state metric.
instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf cost 20 instance-id 1
```

ipv6 ospf dead-interval

Use this command to set the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

The dead interval is advertised in hello packets. OSPF compares the dead interval in a received packet to the dead interval configured for the receiving interface. If the intervals do not match, the hello packet is discarded.

Use the no parameter with this command to reset the interval to default.

Command Syntax

```
ipv6 ospf dead-interval <1-65535>
ipv6 ospf dead-interval <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf dead-interval
no ipv6 ospf dead-interval instance-id (<0-31>|<64-95>)
```

Parameters

`dead-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf dead-interval 20
```

ipv6 ospf demand-circuit

Use this command to enable Hello Suppression and LSA Suppression sent on OSPFv3 interface

Note: Hello's and LSA's will be suppressed on Point-to-point and Point-to-multipoint links and only LSA's will be suppressed for Broadcast link

Use the no parameter with this command to disable Hello Suppression and LSA Suppression.

Command Syntax

```
ipv6 ospf demand-circuit (instance-id (<0-31>|<64-95>))
no ipv6 ospf demand-circuit  (instance-id (<0-31>|<64-95>))
```

Parameters

instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 ospf demand-circuit

(config-if)#no ipv6 ospf demand-circuit
```

ipv6 ospf display route single-line

Use this command to display the output of the show ipv6 ospf route command with each route entry in a single-line.

Use the no parameter with this command to display the output with each route entry in a multiple lines.

Command Syntax

```
ipv6 ospf display route single-line
no ipv6 ospf display route single-line
```

Parameters

None

Default

By default, show ipv6 ospf route displays routes in multiple lines

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf display route single-line
```

ipv6 ospf hello-interval

Use this command to specify the interval between `hello` packets.

The hello interval is advertised in the hello packets. An OSPF router compares the hello interval in a received packet to the interval configured for the receiving interface. If this interval does not match, the hello packet is discarded. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.

Use the `no` parameter with this command to reset the interval to default.

Command Syntax

```
ipv6 ospf hello-interval <1-65535>
ipv6 ospf hello-interval <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf hello-interval
no ipv6 ospf hello-interval instance-id (<0-31>|<64-95>)
```

Parameters

`hello-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf hello-interval 5 instance-id 1
```

ipv6 ospf link-lsa-suppression

Use this command to enable or disable link LSA (type 8) suppression. A type 8 LSA gives information about link-local addresses and a list of IPv6 addresses on the link.

If enabled and the interface type is *not* broadcast or NBMA, the router does not send type 8 link LSAs. This implies that other routers on the link determine the router's next-hop address using a mechanism other than the type 8 link LSA. This feature is implicitly disabled if the interface type is broadcast or NBMA.

Command Syntax

```
ipv6 ospf link-lsa-suppression (enable|disable)
ipv6 ospf link-lsa-suppression (enable|disable) instance-id (<0-31>|<64-95>)
```

Parameters

`enable`	Enable type 8 link LSA suppression
`disable`	Disable type 8 link LSA suppression (default).
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, type 8 link LSA suppression is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf link-lsa-suppression enable
```

ipv6 ospf mtu

Use this command to set MTU size for OSPFv3 to construct packets based on this value. Whenever OSPFv3 constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPFv3 to use the specified value overriding the actual interface MTU size.

Use the no parameter with this command to return to the default value.

Command syntax

```
ipv6 ospf mtu <1280-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf mtu instance-id (<0-31>|<64-95>)
```

Parameters

<1280-65535>	Interface MTU value from OSPFv3's perspective.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, OSPFv3 uses interface MTU derived from the kernel and Instance ID as 0 if not configured.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth1
(config-if)#ipv6 ospf mtu 1287 instance-id 10
```

ipv6 ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the no form of this command to make OSPF check the MTU size during DD exchange.

Command syntax

```
ipv6 ospf mtu-ignore
ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>)
no ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>)
```

Parameters

<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth1
(config-if)#ipv6 ospf mtu-ignore
```

ipv6 ospf neighbor

Use this command to connect OSPFv3 routers to non-broadcast multi-access (NBMA) networks.

One neighbor entry must be included for each known NBMA neighbor. The neighbor address must be a link-local address.

Note: For point-to-multipoint interfaces, the `cost` parameter is the only applicable option.

Use the `no` parameter with this command to remove a configuration.

Command Syntax

```
ipv6 ospf neighbor X:X::X:X (instance-id (<0-31>|<64-95>)|)
ipv6 ospf neighbor X:X::X:X {cost <1-65535>} (instance-id (<0-31>|<64-95>)|)
ipv6 ospf neighbor X:X::X:X {poll-interval <0-4294967295>|priority <0-255>}
  (instance-id (<0-31>|<64-95>)|)
no ipv6 ospf neighbor X:X::X:X ({cost <1-65535>}|{poll-interval <0-
  4294967295>|priority <0-255>}|) (instance-id (<0-31>|<64-95>)|)
```

Parameters

`X:X::X:X`	Specify a neighbor IP address.
`instance-id`	Specify the instance.
`<0-255>`	Specify the instance ID.
`cost`	Cost of the interface. This parameter does not apply to NBMA networks.
`<1-65535>`	Cost of the interface.
`poll-interval`	Dead neighbor polling interval.
`<0-4294967295>`	Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval.
`priority`	Specify a priority. This parameter does not apply to point-to-multipoint interfaces.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

Default cost is 10.

Default poll interval is 120 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```

```
(config)#interface eth0
(config-if)#ipv6 ospf neighbor 2000:500::1 cost 2 instance-id 3
```

ipv6 ospf network

Use this command to set an OSPFv3 network type.

Use the no option with this command to return to the default value.

Command Syntax

```
ipv6 ospf network (broadcast|non-broadcast|point-to-multipoint (non-
  broadcast|)|point-to-point) (instance-id (<0-31>|<64-95>)|)
no ipv6 ospf network (broadcast|non-broadcast|point-to-multipoint (non-
  broadcast|)|point-to-point) (instance-id (<0-31>|<64-95>)|)
```

Parameters

`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`non-broadcast`	Sets the network type to NBMA.
`point-to-point`	Sets the network type to point-to-point.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf network is broadcast type

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the network to point-to-point type on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf network point-to-point
```

ipv6 ospf priority

Use this command to set the router priority for determining the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the no parameter with this command to reset the value to default.

Command Syntax

```
ipv6 ospf priority <0-255>
ipv6 ospf priority <0-255> instance-id (<0-31>|<64-95>)
no ipv6 ospf priority instance-id (<0-31>|<64-95>)
```

Parameters

priority	Specify the router priority of the interface.
<0-255>	Specify the router priority of the interface. The default is 1.
instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, priority is 1

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf priority 127
```

ipv6 ospf retransmit-interval

Use this command to set the interval between retransmission of Link State Update packets. This interval is also used to retransmit DD packets and Link State Request packets.

After sending an LSA to a neighbor, the router keeps the LSA on the LS-retransmission list until it receives an acknowledgement. If the router does not receive an acknowledgment from the neighbor during the retransmit interval, it sends the LSA to the neighbor again.

Use the no parameter with this command to reset the interval to the default value.

Command Syntax

```
ipv6 ospf retransmit-interval <1-1800>
ipv6 ospf retransmit-interval <1-1800> instance-id (<0-31>|<64-95>)
no ipv6 ospf retransmit-interval
no ipv6 ospf retransmit-interval instance-id (<0-31>|<64-95>)
```

Parameters

retransmit-interval	
	Specify the interval.
<1-1800>	Specify the interval in seconds.
instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf retransmit-interval 3
```

ipv6 ospf transmit-delay

Use this command to set the estimated time it takes to transmit a Link State Update packet over the interface. The transmit-delay value is added to the LS age of LSAs and is advertised through this interface whenever the LSAs are transmitted.

Use the no parameter with this command to reset the delay to the default value.

Command Syntax

```
ipv6 ospf transmit-delay <1-1800>
ipv6 ospf transmit-delay <1-1800> instance-id (<0-31>|<64-95>)
no ipv6 ospf transmit-delay
no ipv6 ospf transmit-delay instance-id (<0-31>|<64-95>)
```

Parameters

`transmit-delay`	Specify the time to transmit a link-state update.
`<1-1800>`	Specify the time in seconds to transmit a link-state update.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf transmit-delay 2
```

ipv6 router ospf

Use this command to enable OSPFv3 routing on an interface.

Specify the process ID to configure multiple instances of OSPFv3. When running a single instance of OSPFv3, you do not need to specify a instance ID.

When OSPFv3 receives a packet, it checks if the instance ID in the packet matches the instance ID of the receiving interface.

Use the no parameter with this command to disable OSPFv3 routing on an interface.

Command Syntax

```
ipv6 router ospf area (A.B.C.D|<0-4294967295>)
ipv6 router ospf area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD
ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-95>)
ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>)
ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-95>)
no ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>)
no ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
```

Parameters

area	OSPF Area ID in IPv4 address format.
A.B.C.D	OSPF area ID in IP address format.
<0-4294967295>	OSPF area ID as a decimal value.
instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.
tag	Tag value to use as a “match” value for controlling redistribution via route maps.
WORD	Set the tag value.

Default

By default, ipv6 router ospf is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router ospf area 1 tag Tag1 instance-id 1
```

ipv6 te-metric

Use this command to set the traffic engineering metric for an interface.

The traffic engineering metric is used in OSPF-TE Link State Advertisements. If the traffic engineering metric is not set, the ipv6 ospf cost value for an interface is used in OSPF-TE Link State Advertisements.

Use the no parameter with this command to unset the traffic engineering metric for this interface.

Command Syntax

```
ipv6 te-metric <1-65535>
ipv6 te-metric <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 te-metric instance-id (<0-31>|<64-95>)
```

Parameters

te-metric	Specify the TE metric.
<1-65535>	Specify the TE metric value.
instance-id	Specify the instance.
<0-31>	Interface instance ID for IPv6 unicast
<64-95>	Interface instance ID for IPv4 unicast.

Default

By default, traffic engineering metric value is 0

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 te-metric 6
```

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPFv3 adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPFv3 instance, thus allowing for all of the adjacencies to come up.

Use the no option with this command to remove the limit.

Command Syntax

```
max-concurrent-dd <1-65535>
no max-concurrent-dd
```

Parameters

`<1-65535>`	Specify the number of DD processes.

Default

By default, number of maximum concurrent DD processes is 5

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#max-concurrent-dd 4
```

passive-interface

Use this command to suppress sending Hello packets on all interfaces, or on a specified interface.

This command configures OSPFv3 on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPFv3 does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the `no` form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Command Syntax

```
passive-interface (IFNAME |)
no passive-interface (IFNAME |)
```

Parameters

`IFNAME`	Specify an interface name

Default

By default, passive interface is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#passive-interface eth0
```

redistribute

Use this command to import routes from other routing protocols, or from another OSPF instance, into OSPFv3 AS-external-LSAs.

OSPFv3 advertises routes learned from other routing protocols or from other OSPF instances, including static or connected routes. Each injected prefix is put into the AS-external-LSA with a specified metric and metric-type.

Use the no parameter with this command to stop redistribution.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-65535>|)) {metric
  <0-16777214>|metric-type (1|2)|?route-map WORD|tag <0-4294967295>}
no redistribute(kernel|connected|static|rip|bgp|isis|ospf (WORD|))
```

Parameters

`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF routes.
`WORD`	Specify an OSPFv3 Process Tag. If not specified, redistribute OSPF process with tag "null".
`<1-65535>`	Specify an OSPF process identifier. If not specified, redistribute OSPF instance with process ID 0.
`metric`	Specify the external metric.
`<0-16777214>`	Specify the external metric.
`metric-type`	Specify the external metric-type (see RFC 3101):
`1`	Set OSPF External Type 1 metric.
`2`	Set OSPF External Type 2 metric.
`route-map`	Specify a route map reference.
`WORD`	Specify name of the route-map.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps
`<0-4294967295>`	Specify the route tag.

Default

By default, redistribute is disabled

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows redistribution of BGP routes into the OSPFv3 routing table, with the metric as 10.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#redistribute bgp metric 10 metric-type 1
```

The following example shows redistribution of static IPv4 routes into the OSPFv3 routing table.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#address-family ipv4 unicast
(config-router-af)#redistribute static
(config-router-af)#exit-address-family
```

router-id

Use this command to specify a router ID for the OSPFv3 process.

Configure each router with a unique router-id. In an OSPFv3 router process that has active neighbors, a new router-id is used at the next reload or when you start the OSPFv3 manually.

Use the no form of this command to force OSPFv3 to stop the routing functionality.

Command Syntax

```
router-id A.B.C.D
no router-id (A.B.C.D|)
```

Parameters

A.B.C.D	Specify the router ID in IPv4 address format.

Default

By default, router id is loop-back IP address of IP address with highest IP

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows a fixed router ID 43.3.3.3

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#router-id 43.3.3.3
```

router ipv6 ospf

Use this command to initiate OSPFv3 routing process and enter Router mode to configure OSPFv3 routing process. For making the OSPFv3 routing process functional, you must specify OSPFv3 process tag in router mode and enable OSPFv3 on at least one interface. OSPFv3 is only enabled on interfaces where OSPFv3 process tag matches the tag specified using ipv6 router ospf area command in Interface mode.

Use the no parameter with this command to remove OSPFv3 process.

Command Syntax

```
router ipv6 ospf
router ipv6 ospf WORD
router ipv6 vrf ospf WORD
no router ipv6 ospf
no router ipv6 ospf WORD
no router ipv6 vrf ospf WORD
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.
vrf	Enable an IPv6 VRF routing process

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf Tag1
(config-router)#
```

show debugging ipv6 ospf

Use this command to display the OSPFv3 debugging options.

Command Syntax

```
show debugging ipv6 ospf
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ipv6 ospf

OSPFv3 debugging status:
 OSPFv3 all packet debugging is on
 OSPFv3 all NFSM debugging is on
#
```

show ipv6 ospf

Use this command to display global and area information about OSPFv3.

Command Syntax

```
show ipv6 ospf (WORD|)
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospf
Routing Process "OSPFv3 0" with ID 1.2.3.4
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval
5 secs,
Minimum LSA arrival 1 secs Number of external LSA 3. Checksum Sum 0x2CD6F
Number of areas
in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum 0x2A6AC
```

Table 3-1 explains the fields for each ospf entry.

Table 3-1: show ipv6 ospf output details

Field	Description
Area	Number of areas in device, area addresses, and so on.
Interface attached to this area	The device interfaces attached to the area.
SPF algorithm executed is N	The number of times (N) the OSPF Shortest Path First (SPF) algorithm is executed within the area.
Number of Area scoped LSAs is N	Number of LSAs (N) with a scope of the specified area.
SPF last updated	The interval in seconds that the SPF algorithm was last executed within the area.
Router	Number of router LSAs in the area.
Hold time	Minimum hold time between consecutive SPF calculations.
Checksum	LSA header checksum.

show ipv6 ospf database

Use this command to display information in the OSPFv3 Link State database.

Command Syntax

```
show ipv6 ospf database
show ipv6 ospf database (self-originate|max-age|adv-router A.B.C.D|)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace) (self-originate|adv-router A.B.C.D|)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace) A.B.C.D (self-originate|adv-router A.B.C.D|)
show ipv6 ospf WORD database
show ipv6 ospf WORD database (router|network|inter-prefix|inter-
  router|external|nssa-external|link|intra-prefix|te|grace)
show ipv6 ospf WORD database (router|network|inter-prefix|inter-
  router|external|nssa-external|link|intra-prefix|te|grace) adv-router A.B.C.D
```

Parameters

`self-originate`	Self-originated link states
`max-age`	LSAs in MaxAge list
`adv-router`	Advertising router for Type 8 Link LSAs (Link State Advertisements):
`A.B.C.D`	Router ID of the advertising router.
`router`	Router LSAs.
`network`	Network LSAs.
`inter-prefix`	Inter-Area-Prefix LSAs.
`inter-router`	Inter-Area-Router LSAs.
`external`	AS external LSAs.
`nssa-external`	NSSA LSAs.
`link`	Link LSAs.
`intra-prefix`	Intra-Area-Prefix LSAs (Type 9) with prefixes for stub and transit networks
`te`	Intra-area TE LSAs.
`grace`	Grace LSAs.
`A.B.C.D`	Link state ID as an IP address.
`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: adv-router Parameter

This example shows using the `adv-router` parameter:

```
#show ipv6 ospf database link adv-router 10.70.0.58
            OSPFv3 Router with ID (10.70.0.58) (Process 100)
                Link-LSA (Interface eth1)
  LS age: 492
  LS Type: Link-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0xC2D6
  Length: 68
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: fe80::204:75ff:feaa:fedb
  Number of Prefixes: 2
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Link-LSA (Interface eth1)
```

The router ID and OSPFv3 process tag of the local router.

Interface name of the router associated with this Link-LSA.

OSPFv3 Database Fields

Table 3-2 explains the fields for each database entry.

Table 3-2: OSPFv3 database fields

Field	Description
LS age	The length of time in seconds since the LSA was originated.
LS Type	The type of LSA
Link State ID	Interface identifier of the originating router.
Advertising router	The Router ID of the router advertising this LSA. On a transit network, this is always the Designated Router ID.
LS Seq Number	Sequence number of an LSA.
Checksum	LSA header checksum (excluding the LS age field).
Length	The length in bytes of the LSA (including the 20-byte header).
Priority	The router priority of the interface attaching the originating router of the link.

Table 3-2: OSPFv3 database fields

Field	Description
Options	Bits in network LSAs that originate on the link: DC-bit: Whether the router supports OSPF over Demand Circuits. R-bit: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N-bit: How the router handles Type 7 LSAs. MC-bit: Whether IP multicast packets are forwarded. E-bit: Whether AS-External-LSAs are flooded. This bit is set in all AS External LSAs and in all LSAs. originated in the backbone and non-stub areas. V6-bit: Whether to include the router/link in routing calculations.
Link-Local Address	The originating router's link-local interface address.
Number of Prefixes	The number of IPv6 prefixes associated to the link: Prefix: The global IPv6 prefix associated to this link. Prefix Options: Each prefix is advertised along with an 8-bit capabilities field.They serve as input for routing calculations allowing, for example, some prefixes to be ignored or marked as not re-advertisable.
Referenced LS Type	Identifies the Router-LSA or Network-LSA with which the IPv6 prefixes are associated: Type 0x2001: prefixes associated with Router-LSA Type 0x2002: prefixes associated with Network-LSA
Referenced Link State ID	Referenced LS Type 0x2001: this field is 0 Referenced LS Type 0x2002: the interface ID of the link's Designated Router.
Referenced Advertising Router	Referenced LS Type 0x2001: ID of the originating router. Referenced LS Type 0x2002: ID of the Designated Router Prefix: Referenced LS Type 0x2001: global IPv6 prefix associated with the router Referenced LS Type 0x2002: global IPv6 prefix associated with the transit link Prefix Options: Bits in network LSAs that originate on the link: DC: How the router handles demand circuits R: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N: How the router handles Type 7 LSAs MC: Whether IP multicast packets are forwarded E: Whether AS-External-LSAs are flooded V6: Whether to include the router/link in routing calculations Metric: The cost of this prefix.

Example: intra-prefix and adv-router Parameters

This example shows using the `adv-router` and `intra-prefix` parameters.

Note: The same information for OSPFv2 can be viewed in type 1 router LSAs and type 2 network LSAs. However, in OSPFv3 all addressing information has been removed from router LSAs and network LSAs, leading to the introduction of the Intra-Area-Prefix LSA. In a transit network, the Intra-Area-Prefix-LSA serves the same purpose as a network LSA and on a point-to-point or point-to-multipoint network serves the same purpose as a router LSA.

```
#show ipv6 ospf database intra-prefix adv-router 10.70.0.58
           OSPFv3 Router with ID (10.70.0.58) (Process 100)
```

```
               Intra-Area-Prefix-LSA (Area 0.0.0.0)
  LS age: 1435
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0x1B4E
  Length: 56
  Number of Prefixes: 2
  Referenced LS Type: 0x2002
  Referenced Link State ID: 0.0.0.3
  Referenced Advertising Router: 10.70.0.58
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
    Prefix: 6f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

- The router ID and OSPFv3 process tag for the router.
- Intra-Area-Prefix-LSA has area flooding scope. This LSA belongs to Area 0.0.0.0.

show ipv6 ospf interface

Use this command to display OSPFv3 interface information.

Command Syntax

```
show ipv6 ospf interface
show ipv6 ospf interface IFNAME
```

Parameters

IFNAME	The name of the interface.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

This is a sample output from the `show ipv6 ospf interface` command displaying the OSPFv3 interface information:

```
#show ipv6 ospf interface
eth0 is up, line protocol is up
  Interface ID 3, Instance ID 0, Area 0.0.0.0
  IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
 Router ID 1.2.3.4, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State Backup, Priority 1
 Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e
 Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
 Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
 Neighbor Count is 1, Adjacent neighbor count is 1
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf interface
eth1 is up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::5054:ff:fef3:f166/64 (Link-Local Address)
    2001::2/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 66
    Router ID 2.2.2.2, Network Type P2MP-NBMA, Cost: 1, TE Metric: 1
    Reduce LSA Flooding
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    Timer interval configured, Hello 30, Dead 120, Wait 120, Retransmit 5
      Hello due in 00:00:32
    Neighbor Count is 1, Adjacent neighbor count is 1
    Suppress hello for 1 neighbor(s)
```

```
        Hello received 2 sent 3, DD received 4 sent 6
        LS-Req received 1 sent 1, LS-Upd received 7 sent 4
        LS-Ack received 0 sent 3, Discarded 0
```

Table 3-3 explains the fields for each ospf interface entry.

Table 3-3: show ipv6 ospf interface output details

Field	Description
Interface Type and whether it is up or down.	Status of the interface type.
Line protocol	Status of the line protocol.
Interface ID	Interface for which information is displayed.
Instance ID	For running multiple instances of OSPFv3 on the router
Area	Area ID in A.B.C.D form
IPv6 Link-Local Address	link-local address is an IPv6 unicast address – cannot communicate to link-local addresses that are outside the directly connected network. In IPv6 (X:X::X:X/M) form.
Router ID	As stated – In A.B.C.D form.
Network Type	One of the following: 1. Ethernet is Broadcast 2. Serial p2p non-broadcast 3. NBMA – Non-Broadcast MultiAccess (NBMA) media
cost	The cost of sending packets over this interface – range is 1 to 65535.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1.
Priority	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
Designated Router (ID)	The ID number of the Designated Router (DR).
Interface Address	The IPV6 address of this device.
Backup Designated Router	The ID number or the Backup Designated Router (BDR).
Interface Address	The IPv6 address of the Backup Designated Router.
Timer interval configured	The timer values of the following instances: Hello, Dead, Wait, Retransmit.
Hello due in	The countdown for receiving the next Hello packet.
Neighbor Count is	Number of neighbor count.
Adjacent neighbor count is	Number of adjacent neighbor count.

show ipv6 ospf neighbor

Use this command to display information about an OSPFv3 neighbor.

Command Syntax

```
show ipv6 ospf neighbor
show ipv6 ospf WORD neighbor
show ipv6 ospf neighbor INTERFACE
show ipv6 ospf WORD neighbor INTERFACE
show ipv6 ospf neighbor INTERFACE detail
show ipv6 ospf WORD neighbor INTERFACE detail
show ipv6 ospf neighbor detail
show ipv6 ospf WORD neighbor detail
show ipv6 ospf neighbor A.B.C.D
show ipv6 ospf WORD neighbor A.B.C.D
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.
INTERFACE	Display the name of the Interface
A.B.C.D	Neighbor IP address.
detail	Details of neighbors

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the show ipv6 ospf neighbor command displaying information about the OSPFv3 neighbor.

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID Pri State Dead Time Interface Instance ID
5.6.7.8 1 Full/DR 00:00:38 eth0 0
```

If Hello Suppression is enabled

```
RTR_B#
RTR_B#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/ -         inactive    eth1       0
4.4.4.4           1   Full/DR         00:00:40    eth2       0
4.4.4.4           1   Full/ -         inactive    VLINK1     0
```

```
RTR_B#

RTR_B#
RTR_B#show ipv6 ospf neighbor detail
 Neighbor 1.1.1.1, interface address fe80::5054:ff:feb3:d3bc
    In the area 0.0.0.0 via interface eth1
    Neighbor priority is 1, State is Full, 7 state changes
    Hello is suppressed
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000133 (AF|*|*|DC|R|-|-|E|V6)
    Dead timer due in inactive
    Database Summary List 0
    Link State Request List 0
```

Table 3-4 explains the fields for each ospf neighbor entry.

Table 3-4: show ipv6 ospf neighbor output details

Field	Description
Neighbor	Router ID of the neighbor router.
interface address	IPv6 address of the neighbor's interface.
In the area	The neighbor router's area ID.
via interface	Neighbor router's interface name.
Neighbor Priority is	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
State	The Link State Address (LSA) of the neighbor, and there has been 7 state changes, and sending Hello packets is suppressed.
DR	Designated Router (DR) ID
BDR	Backup Designated Router (BDR) ID
Options is	The hexadecimal representation of the seven bits in the Options Field of Hello packets (see RFC 5340): • AF-bit – Address Family bit. • V6-bit – If this bit is clear, the router/link should be excluded from IPv6 routing calculations. • E-bit – This bit describes the way AS-external-LSAs are flooded. • N-bit – This bit indicates whether or not the router is attached to an NSSA. • R-bit – This bit (the `Router' bit) indicates whether the originator is an active router. If the router bit is clear, then routes that transit the advertising node cannot be computed. Clearing the router bit is appropriate for a multi-homed host that wants to participate in routing, but does not want to forward non-locally addressed packets. • DC-bit – This bit describes the router's handling of demand circuits, as specified in [DEMAND]. • *-bit – These bits are reserved for migration of OSPFv2 protocol extensions.

Table 3-4: show ipv6 ospf neighbor output details (Continued)

Field	Description
Dead timer due in	The countdown timer for marking neighbor connections dead. In this example, the Deat Timer has been deactivated.
Database Summary List	Describes routes to IPv6 address prefixes that belong to other areas.
Link State Request List	Sent or received when Link-State Request packets finds that parts of the Link State Database are out of date.
Timer interval configured	The set values for the following packet types: Hello, Dead, Wait, Retransmit.
Neighbor Count	The number of known neighbors.
Adjacent neighbor count	The number of directly adjacent neighbors.

show ipv6 ospf route

Use this command to display the IPv6 routing table for OSPFv3.

The routes can be displayed in two ways:

- Each routing entry in a single-line
- Each routing entry in multiple lines

By default, the routing table is displayed in the multi-line format. For a single line display, give the ipv6 ospf display route single-line command.

Command Syntax

```
show ipv6 ospf route
show ipv6 ospf WORD route
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is sample output in single-line format:

```
#show ipv6 ospf route
Destination Metric Next-hop
3ffe:1:1::/48 10 directly connected, eth0
3ffe:2:1::/48 10 directly connected, eth0
3ffe:2:2::/48 10 directly connected, eth0
3ffe:3:1::/48 10 directly connected, eth0
3ffe:3:2::/48 10 directly connected, eth0
3ffe:3:3::/48 10 directly connected, eth0
E2 3ffe:100:1::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:2::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:3::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:1::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:2::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:3::/48 20 via fe80::203:47ff:fe4c:776e, eth0
```

The following is sample output in multi-line format:

```
#show ipv6 ospf route
Destination Metric
Next-hop Interface
3ffe:1:1::/48 10
-- eth0
3ffe:2:1::/48 10
-- eth0
3ffe:2:2::/48 10
```

```
-- eth0
3ffe:3:1::/48 10
-- eth0
3ffe:3:2::/48 10
-- eth0
3ffe:3:3::/48 10
-- eth0
E2 3ffe:100:1::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
```

Table 3-5 explains the fields for each ospf route entry.

Table 3-5: show ipv6 ospf route output details

Field	Description
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.

show ipv6 route fast-reroute

Use this command to display loop-free alternate routes with alternate next hops.

Command Syntax

```
show ipv6 route fast-reroute
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

```
#show ipv6 route fast-reroute
```

show ipv6 ospfv3 topology

Use this command to display information about OSPFv3 topology for each area.

Command Syntax

```
show ipv6 ospfv3 topology
show ipv6 ospfv3 WORD topology
show ipv6 ospfv3 topology area (A.B.C.D|<0-4294967295>)
show ipv6 ospfv3 WORD topology area (A.B.C.D|<0-4294967295>)
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.
area	OSPFv3 area ID
A.B.C.D	OSPFv3 Area ID in IPv4 address format.
<0-4294967295>	OSPFv3 Area ID as a decimal value.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospfv3 topology
OSPFv3 paths to Area (0.0.0.0) routers
Router ID Bits Metric Next-Hop Interface
1.2.3.4 --
5.6.7.8 E 10 5.6.7.8 eth0
```

Example

```
#show ipv6 ospfv3 topology

OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
1.2.3.4                                             --
5.6.7.8          E     10         5.6.7.8             eth0
```

Table 3-6 explains the fields for each ospfv3 topology entry.

Table 3-6: show ipv6 ospfv3 topology output details

Field	Description
OSPFv3 path to Area	Area ID in IPv4 format.
Router ID	ID in IPv4 format,

Table 3-6: show ipv6 ospfv3 topology output details

Field	Description
Bits	Bits appended to packets: • V-bit Indicates whether the advertising router is an endpoint of a virtual link. • E-bit Indicates whether the advertising router is an Autonomous System Border Router (ASBR). • B-bit Indicates whether the advertising router is an Area Border Router (ABR). • W-bit When set, the router is a wild-card multicast receiver.
Metric	The value of ospfv3 metric.
Next-Hop	The next-hop identifier.
Interface	The interface name through which the virtual link extends.

show ipv6 ospf virtual-links

Use this command to display information about OSPFv3 virtual-links.

Command Syntax

```
show ipv6 ospf virtual-links
show ipv6 ospf WORD virtual-links
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 4.4.4.4 is up
  Transit area 0.0.0.1 via interface eth2, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 2002::1/128
  Remote address 2002::2/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full
RTR_B#
RTR_B#
```

Table 3-7 explains the fields for each ospf virtual-links entry.

Table 3-7: show ipv6 ospf virtual-links output details

Field	Description
Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IPV6 address and subnet mask.
Remote address	The remote IPv6 address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1. The state is point-to-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ipv6 vrf

Use this command to list information about VRFs.

Command Syntax

```
show ipv6 vrf (WORD|)
```

Parameter

WORD	VPN Routing/Forwarding instance name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output of the `show ipv6 vrf` command displaying VRF information:

```
#show ipv6 vrf
Name             Interfaces

qa               eth0
you              eth1
myVRF            eth2
```

Table 3-8 explains the fields.

Table 3-8: show ipv6 vrf output details

Field	Description
Name	Name of the interface.
Interfaces	Type of an interface.

snmp restart ospf6

Use this command restart SNMP in OSPFv3

Command Syntax

```
snmp restart ospf6
```

Parameter

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart ospf6
```

summary-address

Use this command to summarize or suppress external routes with the specified address range.

An address range is a pairing of a starting address and a mask that is almost the same as IP network number. For example:

- If the specified IPV6 address range is 2020:100:100:2000::/53, it matches 2020:100:100:2222::/64, 2020:100:100:2666::/64 and so on.
- If the specified IPV4 address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Use the no form this command to remove summary addresses.

Command Syntax

```
summary-address X:X::X:X/M (not-advertise|(all-tag (<0-4294967295> ))| )
  (translate-tag (<0-4294967295>) | )
summary-address A.B.C.D/M (not-advertise|tag <0-4294967295>|)
no summary-address A.B.C.D/M
no summary-address X:X::X:X/M (not-advertise|tag (<0-4294967295>|))
no summary-address X:X::X:X/M (not-advertise|(all-tag (<0-4294967295> )) | )
  (translate-tag (<0-4294967295>)| )
no summary-address A.B.C.D/M (not-advertise|tag (<0-4294967295>|))
```

Parameters

`X:X::X:X/M`	The range of addresses given as IPv6 starting address and a mask.
`A.B.C.D/M`	The range of addresses given as IPv4 starting address and a mask.
`not-advertise`	Suppress routes that match the range.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps.
`<0-4294967295>`	Set a tag value. The default is 0.
`all-tag`	Set tag for all summarized type-5, translated type5 and type-7 LSA.
`translate-tag`	Set tag only for summarized translated type-5 LSA.

Default

By default, summary-address value is 0

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#summary-address 2020:100:100:2000::/53 all-tag 3
```

CHAPTER 4 OSPFv3 Graceful Restart Commands

This chapter describes the OSPFv3 graceful restart commands.

capability restart

Use this command to enable OSPFv3 graceful restart capability. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the no parameter with this command to disable the feature.

Command Syntax

```
capability restart graceful
no capability restart
```

Parameter

None

Default

By default, capability restart graceful is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#capability restart graceful

(config)#router ipv6 ospf 100
(config-router)#no capability restart
```

ipv6 ospf restart grace-period

Use this command to enable the graceful restart feature and set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the no parameter with this command to revert to the default grace period.

Command Syntax

```
ipv6 ospf restart grace-period <1-1800>
no ipv6 ospf restart grace-period
```

Parameters

<1-1800>	Grace period in seconds.

Default

By default, grace period is 120 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart grace-period 250
```

ipv6 ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the no parameter with this command to revert to the default.

Command Syntax

```
ipv6 ospf restart helper {max-grace-period <1-1800>}
ipv6 ospf restart helper never (router-id A.B.C.D|)
no ipv6 ospf restart helper
no ipv6 ospf restart helper never
no ipv6 ospf restart helper {max-grace-period|never router-id (A.B.C.D|all)}
```

Parameters

`<1-1800>`	Help only if received grace-period is less than this value.
`A.B.C.D`	Router ID of neighbor to never to act as helper.
`never`	Prevent the neighbor from entering helper mode.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#no ipv6 ospf restart helper never
```

restart ipv6 ospf graceful

Use this command to restart OSPFv3 gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax

```
restart ipv6 ospf graceful (grace-period <1-1800>|)
```

Parameters

<1-1800>	Grace period in seconds.

Default

By default, restart ipv6 ospf graceful is disabled

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart ipv6 ospf graceful grace-period 200
```

CHAPTER 5 OSPF VPN Commands

This chapter provides an alphabetized reference of the OSPF VPN commands. It includes the following commands:

capability vrf-lite

Use this command to enable the `vrf-lite` capability for an OSPF instance.

Use the no parameter with this command to disable the same for an OSPF instance.

Command Syntax

```
capability vrf-lite
no capability vrf-lite
```

Parameters

None

Default

By default, VRF lite capability for an OSPF instance is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf 100
(config-router)#capability vrf-lite
(config)#router ospf 100
(config-router)#no capability vrf-lite
```

router ospf vrf

Use this command to specify a VRF instance in OSPF. To use this command, you must first create a VRF Name in the NSM using the `ip vrf` command. Associate the same name with the OSPF instance using this command.

Command Syntax

```
router ospf <1-65535> WORD
```

Parameters

`<1-65535>`	Routing process ID; should be unique for each routing process.
`WORD`	Name of the VRF to associate with this OSPF instance.

Default

By default, router ospf vrf is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100 myVRF
(config-router)#
```

domain-id

Use this command to specify the domain ID for a OSPF bound to VRF.

The routes sent from OSPF to the VPN cloud are sent along with the domain ID. In this way, the domain ID acts as an identification for the route received from each OSPF domain.

Use the no form of this command to remove a domain ID.

Command Syntax

```
domain-id ((A.B.C.D (secondary|)) | (type (type-as|type-as4|type-back-comp) value HEX_DATA (secondary|)))
no domain-id ((A.B.C.D (secondary|)) | (type (type-as|type-as4|type-back-comp) value HEX_DATA (secondary|)))
```

Parameters

A.B.C.D	Domain ID in IP address format.
secondary	Domain ID is secondary. If not specified the domain ID is primary.
type	Domain type:
type-as	AS format. Hexadecimal value is 0x0005.
type-as4	AS4 format. Hexadecimal value is 0x0205.
type-back-comp	Used for backward compatibility. Hexadecimal value is 0x8000.
value	Domain ID.
HEX_DATA	Domain ID in hexadecimal.
secondary	Domain ID is secondary. If not specified the domain ID is primary

Default

No domain ID is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows configuring a primary domain ID in IP address format.

```
#configure terminal
(config)#router ospf 100 vrf
(config-router)#domain-id 12.12.12.12
```

The following example shows configuring a secondary domain ID in IP address format.

```
#configure terminal
(config)#router ospf 100 vrf
```

```
(config-router)#domain-id 13.13.13.13 secondary
```

The following example shows configuring a primary domain ID in AS type format.

```
#configure terminal
(config)#router ospf 100 vrf
(config-router)#domain-id type type-as value 123456abcdef
```

Intermediate System to Intermediate System Command Reference

Contents

This document contains these chapters:

CHAPTER 1 IS-IS Commands

This chapter describes the IS-IS commands:

- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis lsp-interval
- isis mesh-group
- isis metric
- isis network
- isis password
- isis priority
- isis retransmit-interval
- ispf
- isis wait-timer
- isis wide-metric
- isis tag
- is-type
- key chain
- key
- key-string
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-address
- max-lsp-lifetime
- metric-style
- mpls traffic-eng
- mpls traffic-eng router-id
- net
- passive-interface
- prc-interval-exp
- redistribute
- redistribute isis
- redistribute isis WORD
- router isis
- send-lifetime
- snmp restart isis
- spf-interval-exp
- summary-address

accept-lifetime

Use this command to specify the time period during which the authentication on a key chain is received as valid.

Use the no parameter with this command to negate this command.

Command Syntax

```
accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite
accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite
accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646>
accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646>
no accept-lifetime
```

Parameters

HH:MM:SS	Specify the start time of accept-lifetime in hours, minutes and seconds.
<1-31>	Specify the day of the month to start.
MONTH	Specify the month of the year to start as the first three letters of the month, for example, Jan.
<1993-2035>	Specify the year to start.
HH:MM:SS	Specify the end time of accept-lifetime in hours, minutes and seconds.
<1-31>	Specify the day of the month to end.
MONTH	Specify the month of the year to end as the first three letters of the month, for example, Jan.
<1993-2035>	Specify the year to end.
duration	Indicate the duration parameter.
<1-2147483646>	Specify the actual end time duration of a key in seconds.
infinite	Specify the end time to never expire.

Default

By default, accept-lifetime command is disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of accept-lifetime for key1 on the key chain named mychain.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

address-family ipv6

Use this command to enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.

Use the no parameter with this command to remove all configuration under 'address-family ipv6'.

Command Syntax

```
address-family ipv6 (unicast|)
no address-family ipv6 (unicast|)
```

Parameters

unicast	Specify unicast routing for IPv6.

Default

Unicast routing is not configured.

Command Mode

Router mode

Example

```
#configure terminal
(config)#router isis bb
(config-router)#address-family ipv6 unicast
```

adjacency-check

Use this command to check ISIS neighbor protocol support.

Use the no parameter with this command to uncheck ISIS neighbor protocol support.

Command Syntax

```
adjacency-check
no adjacency-check
```

Parameters

None

Default

By default, adjacency-check command is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis bb
(config-router)#adjacency-check

(config-router)#no adjacency-check
```

area-password

Use this command to set the authentication password for the Level-1 area and to set authentication on Level-1 sequence number PDUs. This command enables authentication when receiving and sending link-state and sequence number PDUs in Level-1 areas. The password must be the same for all the ISIS routers in the same area.

Use the no parameter with this command to clear the area password.

Command Syntax

```
area-password WORD
area-password WORD authenticate snp (send-only|validate)
no area-password
```

Parameters

WORD	Password string.
authenticate	Insert the password into Level-1 SNP PDUs.
snp	Sequence number PDUs.
send-only	Only insert the password into the Level-1 sequence number PDUs, but not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
validate	Insert the password into Level-1 sequence number PDUs and check the password in sequence number PDUs that it receives.

Default

By default, the area password is not configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis bb
(config-router)#area-password mypasswd

(config)#router isis bb
(config-router)#area-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no area-password
```

authentication key-chain

Use this command to set the key chain to be used for authentication at the instance level. Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed.

Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command. If neither the `level-1` nor the `level-2` keyword is configured, the chain applies to both levels. Authentication can be specified for an individual ISIS interface using the `isis authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication.

Command Syntax

```
authentication key-chain WORD (level-1|level-2|)
no authentication key-chain (level-1|level-2|)
```

Parameters

`WORD`	Specify the chain name (valid authentication keys).
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis 1
(config-router)#authentication key-chain myKey level-1
```

authentication mode

Use this command to set the authentication mode at the instance level.

If clear-text authentication was configured using the `area-password` or `domain-password` commands, the `authentication mode` command overrides both of those commands (based on the level at which MD5 is configured). If the `authentication mode` command was used first, and subsequently an attempt is made to use the `area-password` or `domain-password` commands, the attempt fails. To configure clear-text authentication using the `area-password` or `domain-password` commands, first use the `no authentication mode` command.

The type of authentication and the level to which it applies can be specified for a single ISIS interface, rather than per ISIS instance, using the `isis authentication mode` command.

Use the `no` parameter with this command to unset the authentication mode.

Command Syntax

```
authentication mode {md5|text} (level-1|level-2|)
no authentication mode {md5|text} (level-1|level-2|)
```

Parameters

`md5`	Keyed message digest
`text`	Text mode
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The authentication mode is set to MD5 for both levels if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication mode md5 level-1

(config-router)#no authentication mode md5 level-1
```

authentication send-only

Use this command to set the send-only option at the instance level.

Use this command before configuring the authentication mode and authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then, specify the `no authentication send-only` command to disable the send-only feature.

If the `level-1-2` keyword is configured, the send-only feature applies to both levels.

Use the no parameter with this command to unset the send-only option.

Command Syntax

```
authentication send-only (level-1-only|level-2-only|level-1-2)
no authentication send-only
```

Parameters

`level-1-only`	Set send-only option for level-1 only.
`level-2-only`	Set send-only option for level-2 only.
`level-1-2`	Set send-only option for level-1-2

Default

By default, authentication send only is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication send-only level-1

(config-router)#no authentication send-only
```

bfd all-interfaces

Use this command to enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.

This command sets BFD fall-over check for all the neighbors under specified process. To disable BFD checking on particular interface use `isis bfd disable` command at interface mode.

Use the no parameter with this command to disable BFD functionality for an ISIS instance.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

By default, the BFD feature is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis aa
(config-router)#bfd all-interfaces

(config-router)#no bfd all-interfaces
```

capability cspf

Use this command to enable the constrained shortest path first (CSPF) feature in the ISIS module. CSPF calculates optimum explicit route (ER), using Traffic Engineering Database and (TED) and pre-existing Label Switched Path (LSP). The resulting ER is used by a signaling protocol (RSVP-TE) to set up LSPs. Use the no parameter with this command to disable CSPF functionality for an ISIS instance.

Command Syntax

```
capability cspf
no capability cspf
```

Parameters

None

Default

If this command is not used, the CSPF feature is disabled.

Command Mode

Router mode

Example

```
(config)#router isis aa
(config-router)#capability cspf
```

clear clns neighbors

Use this command to clear CLNS neighbor adjacencies.

Command Syntax

```
clear clns neighbors
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>ena
#clear clns neighbors
```

clear clns is-neighbors

Use this command to clear IS neighbor adjacencies.

Command Syntax

```
clear clns is-neighbors System-ID
```

Parameters

`System-ID`	Neighbor system ID in XXXX.XXXX.XXXX format.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#clear clns is-neighbors 1111.1111.1111.1111
```

clear ip isis route

Use this command to clear IPv4 routes.

Command Syntax

```
clear ip isis (WORD|) route (redistribution|all)
```

Parameters

`WORD`	Name that identifies the IS-IS area.
`redistribution`	Clear IS-IS local redistribution routes.
`all`	Clear all of the IS-IS routing tables.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>ena
#clear ip isis route redistribution
```

clear isis adjacency

This command is used to remove the entries from the IS-IS adjacency database. Clears all adjacencies for the specified routing instance or specified interface or particular system ID.

Command Syntax

```
clear isis adjacency (*|IFNAME|system-id XXXX.XXXX.XXXX|) (vrf VRFNAME|)
```

Parameters

*	Clear all neighbors.
IFNAME	Interface name.
XXXX.XXXX.XXXX	Neighbor System-ID.
VRFNAME	VRF name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis adjacency *
```

clear isis counter

Use this command to clear system-wide IS-IS counters (IsisSystemCounterEntry in RFC 4444).

Command Syntax

```
clear isis counter
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis counter
```

clear isis interface counter

Use this command to clear interface counters. If you do not specify a parameter, then counters for all interfaces are cleared.

Command Syntax

```
clear isis interface counter (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis interface counter
```

clear isis process

Use this command to restart ISIS processes. If you do not specify a parameter, then all ISIS processes are restarted.

Command Syntax

```
clear isis (WORD|) process
```

Parameters

WORD	Name that identifies the IS-IS area.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis process
```

debug isis

Use this command to turn on debugging for specified criteria. Debug commands enable to show some debugging information about specified criteria into file or terminal.

Use the no parameter to turn off debugging for specified criteria.

Command syntax

```
debug isis (all|)
debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
no debug isis (all|)
no debug all
no debug all isis
undebug all
undebug isis (all|)
undebug all isis
no debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
undebug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
```

Parameters

`all`	Enables all debugging.
`authentication`	Debugging for authentication.
`checksum`	Debugging for checksums.
`bfd`	Debugging for bidirectional forwarding detection.
`events`	Debugging for internal events.
`hello`	Debugging for hello processing.
`interface`	Interface.
`IFNAME`	Interface name.
`System-ID`	System identifier.
`ifsm`	Debugging for interface finite state machine.
`local-updates`	Debugging for local updates.
`lsp`	Debugging for link-state packet.
`nfsm`	Debugging for neighbor finite state machine.
`nsm`	Debugging for NSM messages.
`pdu`	Debugging for protocol data unit.
`protocol-errors`	Debugging for protocol errors.
`rib`	Debugging for RIB information.

`spf`	Debugging for shortest path first route calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug isis pdu

#configure terminal
(config)#debug isis nsm
```

default-information originate

Use this command to originate reachability information to a default route into link-state packets.

There is no default information in a Level-2 domain by default, while a Level-1 router calculates a default to L1L2 route during SPF calculation. This command originates a default route into a Level-2 domain.

Use the no parameter with this command to withdraw reachability information to a default route from link-state packets.

Command Syntax

```
default-information originate (always| level-1|) (route-map WORD|)
no default-information originate (always| level-1|) (route-map WORD|)
```

Parameters

`originate`	Specify to distribute a default route
`always`	The default route is advertised even if there is no default route in the router's routing table.
`level-1`	Distribute in level-1.
`route-map`	Identifies the level into which the default route is to be announced and can specify other filtering options via a route map.

Default

There is no default information in Level-2 domain by default, while Level-1 router calculates default to L1L2 route during SPF calculation. This command enables to originate default route into Level-2 domain. As an added option, if the user wants to originate the default route in L1 LSP, the "level-1" parameter can be used as follows:

```
default-information originate level-1
```

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#default-information originate
(config-router)#exit
(config)#exit
```

distance (IPv4)

Use this command in router mode to set the administrative distance for all IPv4 routes or routes from a specific source.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance <1-255> (System-ID (WORD|)|)
no distance (System-ID|)
```

Parameters

<1-255>	Distance range.
System-ID	Source ID in XXXX.XXXX.XXXX format.
WORD	Access-list name.

Default

By default, all options are turned off.

Command Mode

Router mode

Examples

The following example shows setting the administrative distance for all routes.

```
#configure terminal
(config)#router isis
(config-router)#distance 10
```

The following example shows setting the administrative distance for a specific route source.

```
#configure terminal
(config)#router isis
(config-router)#distance 40 0000.0000.0001
```

distance (IPv6)

Use this command in router mode to set the administrative distance for all IPv6 routes.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance <1-255>
no distance
```

Parameters

<1-255>	Distance range.

Default

By default, all options are turned off.

Command Mode

Address-family ipv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the administrative distance for all routes.

```
#configure terminal
(config)#router isis
(config-router)#address-family ipv6
(config-router-af)#distance 14
```

domain-password

Use this command to set the authentication password for the Level-2 domain, and optionally, the authentication password on Level-2 sequence number PDUs.

Configuring this command to enable authentication when receiving and sending link state and sequence number PDUs in Level-2 domain. The domain password must be the same in the Level-2 domain.

Use the no parameter with this command to clear the domain password.

Command Syntax

```
domain-password WORD
domain-password WORD authenticate snp (send-only|validate)
no domain-password
```

Parameters

WORD	Password string.
authenticate	Inserts th password into Level-1 sequence number PDUs.
snp	sequence number PDUs.
send-only	Only inserts the password into the Level-1 sequence number PDUs, but does not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
validate	Inserts the password into the Level-1 sequence number PDUs and checks the password in sequence number PDUs received.

Default

By default, there is no domain password.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#domain-password mypasswd

(config)#router isis bb
(config-router)#domain-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no domain-password
```

dynamic-hostname

Use this command to configure the hostname to advertise for an ISIS instance using the dynamic hostname exchange mechanism (RFC 2763) and system-ID-to-hostname translation. This command configures a hostname to use for the Dynamic Hostname Exchange Mechanism and System-ID to hostname translation. This is required to get accurate results when using the show isis database and a few other commands.

Use the no parameter to disable the Hostname configured.

Command Syntax

```
dynamic-hostname
hostname dynamic
dynamic-hostname area-tag
no dynamic-hostname
no hostname dynamic
```

Parameters

area-tag	Use the routing area tag as the hostname, not the router's global hostname.

Default

By default, the Dynamic Hostname Exchange Mechanism is disabled.

Command Mode

Router mode

Example

```
#configure terminal
(config)#router isis bb
(config-router)#dynamic-hostname area-tag
```

fast-reroute per-prefix

Use this command to enable Loop Free Alternate Fast Reroute (LFA FRR) for all prefixes or only those prefixes in a route map.

Use the no form of this command to disable LFA FRR.

Command Syntax

```
fast-reroute per-prefix (level-1|level-2) proto (ipv4) (all|route-map WORD)
 no fast-reroute per-prefix (level-1|level-2) proto (ipv4)
```

Parameters

`level-1`	Level 1 only.
`level-2`	Level 2 only.
`ipv4`	IPv4 address family only.
`all`	All prefixes.
`route-map`	Prefixes from a route map.
`WORD`	Route map name.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute per-prefix level-2 proto ipv4 all
(config-router)#fast-reroute per-prefix level-1 proto ipv4 route-map rmap1
(config-router)#no fast-reroute per-prefix level-2 proto ipv4
```

fast-reroute terminate-hold-on interval

Use this command to set the Loop Free Alternate Fast Reroute (LFA FRR) termination hold-on timer.

Use the no form of this command to set the termination hold-on timer to its default value (1000 milliseconds).

Command Syntax

```
fast-reroute terminate-hold-on interval <100-100000>
no fast-reroute terminate-hold-on interval
```

Parameters

`<100-100000>`	LFA FRR termination hold-on timer interval in milliseconds.

Default

1000 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute terminate-hold-on interval 7000
(config-router)#no fast-reroute terminate-hold-on interval
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path. The tie-breaker value is used to select an LFA FRR route when multiple LFA FRR routes are available for the same primary route.

Use the no form of this command to set the tie-break preference value for a protection type to its default value.

To set all types of repair paths to their default priorities, do not specify a repair path with the no form of this command.

Command Syntax

```
fast-reroute tie-break (level-1|level-2) proto (ipv4) (primary-path|interface-
  disjoint|node-protecting|broadcast-interface-disjoint|secondary-path|downstream-
  path) index <1-255>
no fast-reroute tie-break (level-1|level-2) proto (ipv4) (primary- path|interface-
  disjoint|node-protecting|broadcast-interface-disjoint|secondary-
  path|downstream-path)
```

Parameters

`level-1`	Level 1 only.
`level-2`	Level 2 only.
`ipv4`	IPv4 address family only.
`primary-path`	Use a path from the Equal-Cost Multipath Path (ECMP) set. An ECMP found during the primary shortest path first (SPF) repair might not be desirable in networks where traffic exceeds the capacity of any single link.
`interface-disjoint`	Link protecting: prefer a backup path that uses a different interface than the interface used to reach destination via the primary path.
`node-protecting`	Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path. This ensures complete traffic protection even if the primary next-hop router fails.
`broadcast-interface-disjoint`	Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.
`secondary-path`	Prefer a non-ECMP backup path.
`downstream-path`	Prefer a backup path to the destination which satisfies the downstream condition where the path cost to reach the destination from the LFA next hop is less than the path cost to the destination from the self node via primary next hop: Distance_opt(N, D) < Distance_opt(S, D) This might result in lost traffic, but prevents looping.
`index`	Tie breaking index. A lower value has higher preference.

`<1-255>` Tie breaking index value.

Defaults

`primary-path`	20
`interface-disjoint`	60
`node-protecting`	30
`broadcast-interface-disjoint`	70
`secondary-path`	255
`downstream-path`	90

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute tie-break level-2 proto ipv4 node-protecting
index 127
(config-router)#no fast-reroute tie-break level-1 proto ipv4
broadcastinterface-disjoint
```

ignore-lsp-errors

Use this command to ignore link-state packets (LSPs) with checksum errors. By default, ISIS validates the checksum for LSP and if the checksum has an error, the LSP is dropped. Giving this command says to ignore the LSP checksum error and treat it as if checksum is passed.

Use the no parameter to turn off this function.

Command Syntax

```
ignore-lsp-errors
no ignore-lsp-errors
```

Parameters

None

Default

By default, the LSP checksum is checked on receipt.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In this sample, rtr1 does not drop LSP packets with bad checksum.

```
#configure terminal
(config)#router isis bb
(config-router)#ignore-lsp-errors
```

ip router isis

Use this command to enable ISIS IPv4 routing on the interface. This command is mandatory to ISIS configuration.

After giving this command, the router sends ISIS Hello with IP address TLV on this interface and IP reachability information TLV in link-state packets are updated.

Use the no parameter with this command to disable ISIS IPv4 routing on the interface. This action does not clear the ISIS database. To clear the database, unconfigure the ISIS routing instance.

Command Syntax

```
ip router isis (WORD|)
no ip router isis (WORD|)
```

Parameters

WORD	Name that identifies the IS-IS area. Specify an existing area name or a new area name.

Default

By default, IPv4 routing is disabled on the router.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip router isis bb
```

ipv6 router isis

Use this command to enable ISIS IPv6 routing on the interface. This command is mandatory to IPv6 ISIS configuration. Match the ISIS instance tag to one of existing instance's tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface.

Configuring this command, the router sends ISIS Hello with IPv6 address TLV on this interface, and IPv6 reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable ISIS IPv6 routing on the interface.

Command Syntax

```
ipv6 router isis (WORD|)
no ipv6 router isis (WORD|)
```

Parameters

WORD	ISIS instance name.

Default

By default, IPv6 routing is disabled on the router.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router isis bb
```

isis authentication key-chain

Use this command to set the key chain to be used for authentication on the interface-related packets.

Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the `key-chain` command, no key-chain authentication is performed. Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command.

If neither the `level-1` nor `level-2` keyword is configured, the key chain applies to the level(s) on which the authentication mode is configured as `md5`. Authentication can be specified for an entire instance of ISIS, instead of at the interface level, by using the `authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication on the interface-related packets.

Command Syntax

```
isis authentication key-chain WORD (level-1|level-2|)
no isis authentication key-chain (level-1|level-2|)
```

Parameters

`WORD`	Chain name - valid authentication keys.
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication key-chain myKey level-1
```

isis authentication mode md5

Use this command to set the MD5 authentication mode. If clear text authentication was configured using the `isis password` command, the `isis authentication mode` command overrides the `isis password` command. If the `isis authentication mode` command was used, then subsequently an attempt is made to use the `isis password` command, the attempt fails.

To configure clear text authentication using the `isis password` command, first use the `no isis authentication mode` command. The type of authentication and the level to which it applies can be specified for the entire ISIS instance, rather than per interface, using the `authentication mode` command.

Use the `no` parameter with this command to unset the MD5 authentication mode.

Command Syntax

```
isis authentication mode {md5|text} (level-1|level-2|)
no isis authentication mode {md5|text} (level-1|level-2|)
```

Parameters

`md5`	Keyed message digest
`text`	Text mode
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The authentication mode will be set to MD5 for both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication mode md5 level-1
```

isis authentication send-only

Use this command to set the send-only option to the interface-related packets.

Use this command before configuring the ISIS authentication mode and ISIS authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.

Use the no parameter with this command to unset the send-only option to the interface-related packets.

Command Syntax

```
isis authentication send-only (level-1-only|level-2-only|level-1-2)
no isis authentication send-only
```

Parameters

`level-1-only`	Set send-only option for level-1 only.
`level-2-only`	Set send-only option for level-2 only.
`level-1-2`	Set send-only option for level-1-2

Default

By default, this option is disabled. The send-only option applies to both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication send-only level-1-only
```

isis bfd

Use this command to enable/disable the BFD check on interface.

The `isis bfd` command allows a user to enable BFD on an interface. The `isis bfd disable` command disables BFD checking on an interface. However, the `no isis bfd` and `no isis bfd disable` commands both remove the enable/disable configuration, but do not disable/enable BFD.

The `bfd all-interfaces` command enables BFD on all interfaces attached to an instance then configuring. This command disables BFD configuration on a particular interface.

Command Syntax

```
isis bfd (disable|)
no isis bfd (disable|)
```

Parameters

`disable`	Specify to disable BFD.

Default

By default, bfd feature enable/disable is not configured.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis bfd disable
```

isis circuit-type

Use this command to set the circuit type for the interface.

If level-1 or level-2-only is specified in this command, ISIS sends only the specified level of PDUs. On the point-to-point interface, there is only one type of Hello packet, so in this case ISIS Hello will be sent regardless of circuit-type. If is-type is configured as level-1 or level-2 only, routing for this instance is performed for only the specified level. In this manner, only the particular level of PDU is sent on the interface.

Use the no parameter to reset circuit type to the default.

Command Syntax

```
isis circuit-type (level-1|level-1-2|level-2-only)
no isis circuit-type
```

Parameters

`level-1`	Specify that only Level-1 adjacencies are formed.
`level-1-2`	Specify that Level-1-2 adjacencies are formed.
`level-2-only`	Specify that only Level-2 adjacencies are formed.

Default

By default, the default circuit-type is level-1-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis circuit-type level-2-only
```

isis csnp-interval

Use this command to set CSNP (Complete sequence number PDU) interval in seconds.

Configuring this command changes the interval between two consecutive CSNP transmission. By default, CSNP is sent every 10 seconds only by LAN DIS. This parameter is only valid on broadcast interface, since periodic CSNP is only sent on broadcast interface, while CSNP on Point-to-Point interface is sent only when adjacency is initiated.

Use the `no` parameter with this command to reset CSNP interval to the default value.

Command Syntax

```
isis csnp-interval <1-65535> (level-1|level-2|)
no isis csnp-interval (level-1|level-2|)
```

Parameters

`<1-65535>`	Specify the CSNP interval in seconds.
`level-1`	Specify Level-1 CSNP.
`level-2`	Specify Level-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis csnp-interval 20
```

isis fast-reroute per-prefix candidate disable

Use this command to prevent an interface from becoming an Loop Free Alternate Fast Reroute (LFA FRR) for a primary route.

Use the no form of this command to enable an interface to become an LFA FRR for a primary route.

Command Syntax

```
isis fast-reroute per-prefix candidate disable (level-1|level-2)
no isis fast-reroute per-prefix candidate disable (level-1|level-2)
```

Parameters

`level-1`	Level-1 only
`level-2`	Level-2 only

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis fast-reroute per-prefix candidate disable level-2
(config-if)#no isis fast-reroute per-prefix candidate disable level-2
```

isis hello-interval

Use this command to set the Hello interval in seconds. The Hello-interval is set with the hello-multiplier (see `isis hello-multiplier` command).

Configuring this command changes the time interval between two consecutive Hello transmissions. If a device receives its own LSP with a maximum sequence number, then it suspends ISIS for the hold interval. DIS sends Hello transmissions at three times the rate than non-DIS. If ISIS is elected as DIS on this interface, ISIS sends Hello every 3.3 seconds.

If `minimal` keyword is specified, Holding timer in Hello PDU is set to 1 second and Hello interval is calculated by dividing by the hello-multiplier. For example, if the hello-multiplier is configured as 4 and `hello-interval minimal` is the command used, an Hello PDU is sent every 250 milliseconds.

Use the `no` parameter to set the Hello interval to the default.

Command Syntax

```
isis hello-interval <1-65535> (level-1|level-2|)
isis hello-interval minimal (level-1-only|level-2-only|level-1-2)
no isis hello-interval (level-1|level-2|)
no isis hello-interval minimal
```

Parameters

`<1-65535>`	Specify the hello interval in seconds.
`minimal`	Specify the holding-time as 1 second.
`level-1`	Specify Level-1 CSNP.
`level-2`	Specify Level-2 CSNP.
`level-1-only`	Specify only Level-1 CSNP.
`level-2-only`	Specify only Level-2 CSNP.
`level-1-2`	Specify both Level-1 and Level-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-interval 5 level-1

(config-if)#isis hello-interval minimal level-1-only
```

isis hello-multiplier

Use this command to set multiplier for Hello holding time.

Changes Holding Timer in Hello PDU. Holding timer is calculated by “Hello-Interval” multiplied by this value. If `minimal` keyword is specified with the Hello-Interval, the holding timer is set to 1 second and the hello-interval is calculated by dividing 1 by this value.

Use the `no` parameter with this command to set multiplier to the default.

Command Syntax

```
isis hello-multiplier <2-100> (level-1|level-2|)
no isis hello-multiplier (level-1|level-2|)
```

Parameters

`<2-100>`	Specify a hello multiplier value.
`level-1`	Specify Level-1 hello.
`level-2`	Specify Level-2 hello.

Default

By default, ISIS uses 3 seconds for the multiplier value and the multiplier is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-multiplier 4
```

isis hello padding

Use this command to enable IS-IS hello padding at the interface level.

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

Use the `no` parameter with this command to disable IS-IS hello padding.

Command Syntax

```
isis hello padding
no isis hello padding
```

Parameters

None

Default

By default, ISIS hello padding is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#isis hello padding

(config-if)#no isis hello padding
```

isis lsp-interval

Use this command to set the link-state packet (LSP) transmission interval.

Giving this command changes the minimum interval between two consecutive LSP transmission. When flooding or some other event triggers LSP transmission, the LSP is put in the interface queue and scheduled to send according to this interval. Two consecutive LSP transmissions are scheduled to have at least this interval.

Use the no parameter with this command to set LSP transmission interval to the default.

Command Syntax

```
isis lsp-interval <1-4294967295>
no isis lsp-interval
```

Parameters

`<1-4294967295>` LSP transmission interval in milliseconds.

Default

By default, ISIS uses 33 milliseconds for the interval.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis lsp-interval 100

(config-if)#no isis lsp-interval
```

isis mesh-group

Use this command to set Mesh Group ID on the current interface.

Use the no parameter to unset mesh group on the current interface.

Command Syntax

```
isis mesh-group <1-4294967295>
no isis mesh-group
```

Parameters

`<1-4294967295>` Specify a mesh group number

Default

By default, mesh groups are not enabled on this interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#isis mesh-group 20

(config)#interface eth2
(config-if)#no isis mesh-group
```

isis metric

Use this command to set the default metric for the interface. The interface default metric is put into IP reachability information TLVs and in IS reachability information TLVs in link-state packets. The value is used for SPF calculation, and is applied when the metric-style is configured as “narrow”.

Use the no parameter with this command to set default metric to the default.

Command Syntax

```
isis metric <1-63> (level-1|level-2|)
no isis metric (level-1|level-2|)
```

Parameters

<1-63>	Default metric.
level-1	Default metric for level-1 circuit.
level-2	Default metric for level-2 circuit.

Default

By default, ISIS uses 10 for the metric value and the value is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis metric 20
```

isis network

Use this command to change a broadcast interface network type to a point-to-point network type.

Use the no parameter with this command to revert to the default setting of a broadcast interface network type.

Command Syntax

```
isis network (broadcast|point-to-point)
no isis network
```

Parameters

broadcast	Specify ISIS a broadcast multi-access network.
point-to-point	Specify ISIS a point-to-point network.

Default

By default, the network is set to a broadcast multi-access network type.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis network point-to-point
```

isis password

Use this command to set the authentication password of Hello PDU on the interface.

Use the no parameter to clear the password.

Command Syntax

```
isis password WORD (level-1|level-2|)
no isis password (level-1|level-2|)
```

Parameters

WORD	Specify a password string.
level-1	Specify a password for Level-1 hello PDUs.
level-2	Specify a password for Level-2 hello PDUs.

Default

By default, no password is configured; this applies to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis password mypassword level-1
```

isis priority

Use this command to set the priority for LAN DIS election. This command changes the priority value in LAN ISIS Hello PDUs. A lower priority value is less preferred in DIS election, and a higher priority value is more preferred.

Note: This command is not valid for Point-to-Point interface.

Use the no parameter to set priority to the default.

Command Syntax

```
isis priority <0-127> (level-1|level-2|)
no isis priority (level-1|level-2|)
```

Parameters

<0-127>	Priority value
level-1	Specify a password for Level-1 hello PDUs.
level-2	Specify a password for Level-2 hello PDUs.

Default

By default, ISIS uses 64 for the priority value, and the priority is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis priority 127
```

isis retransmit-interval

Use this command to set the link-state packet (LSP) retransmission interval.

Use the no parameter to set the interval to the default.

Command Syntax

```
isis retransmit-interval <1-65535>
no isis retransmit-interval
```

Parameters

<1-65535>	Interval for retransmission of the same LSP in seconds.

Default

By default, ISIS uses an interval of 5 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis retransmit-interval 10

(config-if)#no isis retransmit-interval
```

ispf

Use this command to enable incremental SPF for a routing process.

Use the no parameter to disable incremental SPF from a routing process.

Command Syntax

```
ispf (level-1|level-1-2|level-2-only)
no ispf
```

Parameters

level-1	Act as level-1 only IS.
level-1-2	Act as level-1-2 IS.
level-2-only	Act as level-2 only IS.

Default

By default, all levels are turned off.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#ispf level-1

(config)#router isis bb
(config-router)#no ispf
```

isis wait-timer

Use the isis wait-timer seconds command to configure the number of seconds the router will wait for adjacency information

Use the no parameter to set the wait-timer to the default.

Command Syntax

```
isis wait-timer <1-65535> (level-1|level-2|)
no isis wait-timer (level-1|level-2|)
```

Parameters

`level-1`	Act as level-1 only IS.
`level-2`	Act as level-2 only IS.

Default

By default, wait-timer will be 20 seconds (2 times the hello timer).

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#isis wait-timer 30

(config)#router isis bb
(config-router)#no isis wait-timer
```

isis wide-metric

Use this command to set wide metric for the interface.

Interface wide-metric is put into Extended IP reachability TLVs. Extended IS reachability TLVs and IPv6 rechability TLVs in LSPs. The value is used for SPF calculation. The value is applied when metric-style is configured as 'wide'.

Use the no parameter to set wide metric to the default.

Command Syntax

```
isis wide-metric <1-16777214> (level-1|level-2|)
no isis wide-metric (level-1|level-2|)
```

Parameters

<1-16777214>	Specify a wide metric.
level-1	Specify the wide metric for Level-1 circuit.
level-2	Specify the wide metric for Level-2 circuit.

Default

By default, ISIS uses 10 for the metric value and the metric is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

None.

Examples

```
#configure terminal
(config)#interface eth0
(config-router)#isis wide-metric 100

(config)#interface eth0
(config-router)#no isis wide-metric 100
```

isis tag

Use this command to sets the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface.

If you do not specify a parameter, then the tag value is set for level-1-2 boundary.

Use the no parameter to unset the tag.

Command Syntax

```
isis tag <1-4294967295> (level-1|level-2|)
no isis tag (level-1|level-2|)
```

Parameters

`<1-4294967295>`	Tag value.
`level-1`	Specify the tag value for the level-1 boundary.
`level-2`	Specify the tag value for the level-2 boundary.

Command Mode

Interface mode

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth0
(config-if)#isis tag 500 level-1
```

is-type

Use this command to set the IS to the specified level of routing.

Changing `is-type` brings down, then brings up a particular level of routing. There is a limitation: Only one ISIS instance can run Level-2 routing (either Level-2 only IS, or Level-1-2 IS).

Use the `no` parameter to set the IS to the default.

Command Syntax

```
is-type (level-1|level-1-2|level-2-only)
no is-type
```

Parameters

`level-1`	Act as level-1 only IS.
`level-1-2`	Act as level-1-2 IS.
`level-2-only`	Act as level-2 only IS.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#is-type level-1

(config)#router isis bb
(config-router)#no is-type
```

key chain

Use this command to enter the key chain management mode and to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax

```
key chain WORD
no key chain WORD
```

Parameters

WORD	Specify the name of the key chain to manage.

Default

By default, keychain mode is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

key

Use this command to manage, add or delete authentication keys in a key-chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax

```
key <0-2147483647>
no key <0-2147483647>
```

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```

key-string

Use this command to define a password to be used by a key.

Use the no parameter with this command to disable this feature.

Command Syntax

```
key-string LINE
no key-string
```

Parameters

LINE	Specify a string of characters to be used as a password by the key.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```

lsp-gen-interval

Use this command to set the minimum interval before regenerating the same link-state packet (LSP). The smaller the interval, the faster the convergence. However, this setting might cause more frequent flooding.

Use the `no` parameter with this command to set the interval to the default.

Command Syntax

```
lsp-gen-interval <1-120>
lsp-gen-interval (level-1|level-2) <1-120>
no lsp-gen-interval (level-1|level-2|)
```

Parameters

`<1-120>`	Minimum interval in seconds.
`level-1`	Interval for Level-1 IS.
`level-2`	Interval for Level-2 IS.

Default

By default, ISIS uses 30 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-gen-interval 5
```

lsp-mtu

Use this command to set maximum transfer unit for link-state packets (LSPs).

Use the no parameter with this command to set the interval to the default.

Command Syntax

```
lsp-mtu (level-1|level-2|) <512-1492>
no lsp-mtu (level-1|level-2|)
```

Parameters

`<512-1492>`	MTU size
`level-1`	Size for Level-1 IS.
`level-2`	Size for Level-2 IS.

Default

By default, the MTU is 1492 bytes.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-mtu 555
```

lsp-refresh-interval

Use this command to set the link-state packet (LSP) refresh interval.

IP Infusion Inc. recommends making the `lsp-refresh-interval` smaller than the max-lsp-lifetime value.

Use the `no` parameter to set the interval to the default value.

Command Syntax

```
lsp-refresh-interval <1-65535>
no lsp-refresh-interval
```

Parameters

`<1-65535>`	Refresh interval in seconds.

Default

By default, the interval is 900 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-refresh-interval 600

(config)#router isis bb
(config-router)#no lsp-refresh-interval
```

max-area-address

Use this command to set the maximum number of ISIS areas that can be configured on this router with the `net` command. By default, ISIS permits a maximum of three areas that can be defined on a router.

Use the `no` parameter with this command to set the maximum number of ISIS areas to its default (3).

Command Syntax

```
max-area-address <3-254>
no max-area-address
```

Parameters

`<3-254>`	The maximum number of areas in the network.

Default

By default, the maximum number of areas is 3.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis net2
(config-router)#max-area-address 5
(config-router)#net 71.0001.0000.0000.0001.00
(config-router)#net 72.0001.0000.0000.0001.00
(config-router)#net 73.0001.0000.0000.0001.00
(config-router)#net 74.0001.0000.0000.0001.00
(config-router)#net 75.0001.0000.0000.0001.00
```

max-lsp-lifetime

Use this command to set the maximum link-state packet (LSP) lifetime. You must set `max-lsp-lifetime` greater than the lsp-refresh-interval interval.

Use the `no` parameter to set the lifetime to the default.

Command Syntax

```
max-lsp-lifetime <350-65535>
no max-lsp-lifetime
```

Parameters

`<350-65535>`	Maximum LSP lifetime in seconds.

Default

By default, max-lsp-lifetime is set to 1200 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#max-lsp-lifetime 1500

(config)#router isis bb
(config-router)#no max-lsp-lifetime
```

metric-style

Use this command to configure the ISIS metric style. Use the following table when changing the method of how TLV encodes and SPF calculates a decision:

Metric-style Command	Wide SPF	Wide TLV	Narrow SPF	Narrow TLV
narrow (default)	OFF	OFF	ON	OFF
narrow transition	ON	OFF	ON	ON
wide	ON	ON	OFF	OFF
wide transition	ON	ON	ON	OFF
transition	ON	ON	ON	ON

Where:

- Wide SPF: Uses wide TLVs for SPF calculation.
- Wide TLV: Encodes wide TLVs in the LSP.
- Narrow SPF: Uses narrow TLVs for SPF calculation.
- Narrow TLV: Encodes narrow TLVs in the LSP.

Use the no parameter to set the style to the default style, narrow.

Command Syntax

```
metric-style (narrow|wide|transition) (level-1|level-2|)
metric-style (narrow|wide) transition (level-1|level-2|)
no metric-style
```

Parameters

`narrow`	Specify the old style of TLVs with narrow metric.
`wide`	Specify the new style of TLVs to carry wider metric.
`transition`	Specify to send and accept both styles of TLVs during transition.
`level-1`	Specify the level-1 metric style.
`level-2`	Specify the level-2 metric style.
`transition`	Accept both styles of TLVs during transition

Default

By default, ISIS uses narrow metric style for level 1 and 2.

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#metric-style narrow transition
```

mpls traffic-eng

Use this command to configure MPLS Traffic Engineering feature for ISIS.

Use the no parameter to turn off the feature.

Note: Metric-style wide must be enabled before using this CLI.

Command Syntax

```
mpls traffic-eng (level-1|level-2)
no mpls traffic-eng (level-1|level-2)
```

Parameters

`level-1`	Specify the level-1 MPLS Traffic Engineering feature.
`level-2`	Specify the level-2 MPLS Traffic Engineering feature.

Default

If this command is not used, ISIS does not encode traffic engineering TLVs and Sub-TLVs.

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#metric-style wide
(config-router)#mpls traffic-eng level-1

(config)#router isis bb
(config-router)#no mpls traffic-eng level-1
```

mpls traffic-eng router-id

Use this command to configure the traffic engineering stable IP address for a system.

Use the no parameter to turn off the feature.

Command Syntax

```
mpls traffic-eng router-id A.B.C.D
no mpls traffic-eng router-id
```

Parameters

A.B.C.D	Specify the ISIS router-ID in an IP address format.

Default

If this command is not used, and traffic engineering is enabled, ISIS will use global router-id..

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#mpls traffic-eng router-id 10.10.0.23

(config)#router isis bb
(config-router)#no mpls traffic-eng router-id
```

net

Use this command to add a Network Entity Title (NET) for the instance.

On a router running ISIS, a NET can be 8 to 20 bytes in length. The last byte is always the n-selector, and must be zero. The n-selector indicates no transport entity, and means that the packet is for the routing software of the system. The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

The bytes preceding the system ID are the area ID, which can be from 1 - 13 bytes in length. By default, a maximum of three NETs per router are allowed with a different area ID but the system ID should be the same for all NETs. You can increase the number of area IDs per system ID with the `max-area-address` command.

Use the `no` parameter to remove the NET.

Command Syntax

```
net NET
no net NET
```

Parameters

`NET`	Specify a network entity title (NET) in 1 to 13 octets (that is, XX.XXXX. ... .XXXX.XX).

Default

By default, ISIS does not configure a NET and routing is not enabled for the interface.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#net 49.0000.0001.0002.0003.00
```

passive-interface

Use this command to suppress routing updates on all interfaces or on a specified interface, which puts the interfaces into passive mode.

To advertise passive prefixes in LSP, an interface must be configured with ip router isis when using "passive-interface" command. If interface is not configured with isis instance "passive-interface IFNAME" command must be used to add that interface as passive. Enabling passive interface on an ISIS enabled interface disables ISIS routing updates on the interface and makes the interface passive.

Use the no parameter with this command to remove interfaces from passive mode

Command Syntax

```
passive-interface (IFNAME |)
no passive-interface (IFNAME |)
```

Parameters

IFNAME	Indicates an interface name. If this parameter is omitted, then all interfaces become passive or active.

Command Mode

Router mode

Examples

The following suppresses routing updates on a specified interface.

```
#configure terminal
(config)#router isis 100
(config-router)#passive-interface eth0
(config)#router isis 100
(config-router)#no passive-interface eth0
```

prc-interval-exp

Use this command to configure exponential back-off delay between PRC calculations.

Use the no parameter to disable any set exponential back-off delay between PRC calculations.

Command Syntax

```
prc-interval-exp
prc-interval-exp <0-2147483647> <0-2147483647>
no prc-interval-exp
```

Parameters

`<0-2147483647>`	Set the minimum delay between receiving a change to PRC calculation in milliseconds.
`<0-2147483647>`	Set the maximum delay between receiving a change to PRC calculation in milliseconds.

Default

By default, minimum delay is 500 milliseconds and maximum delay is 50 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis
(config-router)#prc-interval-exp 100 10000

(config)#router isis
(config-router)#no prc-interval-exp
```

redistribute

Use this command to redistribute routes from another protocol into the ISIS routing table.

Use the no parameter to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|ospf|bgp) {metric <0-16777215>| metric-
  type (internal|external)|level-1|level-2|level-1-2|route-map WORD}
no redistribute (kernel|connected|static|rip|ospf|bgp)  {metric <0-16777215>|
  metric-type (internal|external)|level-1|level-2|level-1-2|route-map WORD}
```

Parameters

kernel	Redistribute kernel routes.
connected	Redistribute connected routes.
static	Redistribute static routes.
rip	Redistribute RIP routes.
ospf	Redistribute OSPF routes.
bgp	Redistribute BGP routes.
metric	Specify the metric for redistributed routes.
<0-16777215>	Specify the IS-IS default metric.
metric-type	Specify the IS-IS exterior metric type for redistributed routes:
internal	Set IS-IS internal metric type.
external	Set IS-IS external metric type.
level-1	Redistribute routes into level 1 only
level-2	Redistribute routes into level 2 only (default)
level-1-2	Redistribute routes into both levels.
route-map	Specify a Route map reference.
WORD	Specify name of the route-map.

Default

By default, redistribute command is disabled.

If no level parameter is specified, by default redistributed routes will be added in level-2 LSP. If is-type of an IS-IS instance is level-1, the level parameter must be set to level-1 for redistribute command to take effect and redistribute routes in L1 LSP.

Command Mode

For Ipv4: Router mode

For Ipv6: address-family ipv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router isis A
(config-router)#redistribute bgp metric 12
```

redistribute isis

Use this command to redistribute reachability information from one level to the other level. If an distribute-list name is given with this command for an access list that does not exist, the routes are still redistributed.

Use the no parameter with this command to stop redistribution.

Command Syntax

```
redistribute isis level-1 into level-2
redistribute isis level-2 into level-1
redistribute isis level-1 into level-2 distribute-list WORD
redistribute isis level-2 into level-1 distribute-list WORD
no redistribute isis level-1 into level-2
no redistribute isis level-2 into level-1
```

Parameters

`level-1`	Specify an inter-area route from level-1.
`level-2`	Specify an inter-area routes from level-2.
`into`	Specify a level from level-n into level-m.
`level-1`	Specify an inter-area route into level-1.
`level-2`	Specify an inter-area routes into level-2.
`distribute-list`	Indicate the distributed-list parameter.
`WORD`	Specify the actual selected route.

Default

By default, ISIS redistributes selected L1 routes into L2.

Command Mode

For Ipv4: Router mode

For Ipv6: address-family ipv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1

(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1 distribute-list new

(config)#router isis bb
(config-router)#no redistribute isis level-2 into level-1
```

redistribute isis WORD

Use this command to redistribute reachability information from one isis instance into another instance. Only one isis instance can be redistributed.

Use the `no` parameter with this command to stop redistribution.

Note: This command is not supported for address family IPv6.

Command Syntax

```
redistribute isis WORD {metric <0-16777215>| metric-type (internal|external)
  |level-1|level-2|level-1-2|route-map WORD}
```

```
no redistribute isis WORD {metric <0-16777215>| metric-type
  (internal|external)|level-1|level-2|level-1-2|route-map WORD}
```

Parameters

`WORD`	Specify an isis instance name or tag
`metric`	Specify the metric for redistributed routes.
`<0-16777215>`	Specify the IS-IS default metric.
`metric-type`	Specify the IS-IS exterior metric type for redistributed routes:
`internal`	Set IS-IS internal metric type.
`external`	Set IS-IS external metric type.
`level-1`	IS-IS Level-1 routes.
`level-2`	IS-IS Level-2 routes.
`level-1-2`	IS-IS Level-1 and Level-2 routes.
`route-map`	Specify a Route map reference.
`WORD`	Specify name of the route-map.

Default

By default, redistribute command is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router isis A
(config-router)#redistribute isis B metric 12
```

router isis

Use this command to initiate an ISIS routing instance. This command starts the ISIS routing instance and enters router configuration mode. Configure at least one NET to start routing. Also, enable a particular interface with the ip router isis command.

Use the no parameter with this command to remove an ISIS routing instance.

Command Syntax

```
router isis WORD
no router isis WORD
```

Parameters

WORD	Name that specifies an ISO routing instance tag.

Default

By default, ISIS routing instance is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis New
(config-router)#
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the no parameter with this command to negate this command.

Command Syntax

```
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646>
no send-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.
`MONTH`	Specify the month of the year to start as the first three letters of the month, for example, Jan.
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to end.
`MONTH`	Specify the month of the year to end as the first three letters of the month, for example, Jan.
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Applicability

No default value is specified

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#send-lifetime 03:03:01 Jan 3 2004 04:04:02 Dec 6 2006
```

snmp restart isis

Use this command to restart SNMP in Intermediate System to Intermediate System (IS-IS)

Command Syntax

```
snmp restart isis
```

Parameters

None

Default

By default, snmp restart is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart isis
```

spf-interval-exp

Use this command to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations.

The `spf-interval-exp` command configures the minimum and maximum interval time between the receipt of a topology change and the calculation of the SPF.

Use the `no` parameter with this command to set the minimum and maximum hold intervals to the default.

Command Syntax

```
spf-interval-exp <0-2147483647> <0-2147483647>
spf-interval-exp (level-1|level-2) <0-2147483647> <0-2147483647>
no spf-interval-exp ((level-1|level-2)|)
```

Parameters

`<0-2147483647>`	Specify the minimum delay between receiving a change to the SPF calculation in milliseconds. The default SPF minimum hold-time interval value is 500 milliseconds.
`<0-2147483647>`	Specify the maximum delay between receiving a change to the SPF calculation in milliseconds. The default SPF maximum hold-time interval value is 50 seconds.
`level-1`	Specify an interval for Level-1 IS.
`level-2`	Specify an interval for Level-2 IS.

Default

By default, ISIS uses 500 milliseconds and 50,000 milliseconds for the minimum and maximum hold intervals, respectively. The values are applied to both level-1 and level-2 if the `level` parameter is omitted.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#spf-interval-exp level-1 600 60000

(config)#router isis bb
(config-router)#no spf-interval-exp level-1
```

summary-address

Use this command to configure Summary Address to summarize IPv4 reachability information.

Use the no parameter with this command to unconfigure the summary.

Command Syntax

```
summary-address A.B.C.D/M (level-1 |level-1-2 |level-2) (metric <1-63>|)
no summary-address A.B.C.D/M
```

Parameters

`A.B.C.D/M`	Specify the IPv4 prefix to be announced.
`level-1`	Specify the reachability information only for Level-1.
`level-1-2`	Specify the reachability information for both Level-1 and Level-2.
`level-2`	Specify the reachability information only for Level-2.
`metric`	Specify the metric for the summarized address.
`<1-63>`	Specify the metric. The default is 0.

Default

By default, ISIS does not configure the summary-address. Level must be configured along with summary-address. Metric is optional.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#summary-address 10.10.0.0/16 level-1-2 metric 3

(config)#router isis bb
(config-router)#no summary-address 10.10.0.0/16
```

CHAPTER 2 IS-IS Graceful Restart Commands

This chapter describes the IS-IS graceful restart commands:

capability restart graceful

Use this command to enable the graceful restart capability.

Use the no parameter with this command to negate this command.

Command Syntax

```
capability restart graceful
no capability restart graceful
```

Parameters

NA

Default

By default, graceful restart capability is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables the graceful restart capability on a router.

```
#configure terminal
(config)#router isis bb
(config-router)#capability restart graceful
```

isis restart grace-period

Use this command to configure the T3 timer, the time the restarting router retains the forwarding table.

Use the no parameter to use the default value.

Command Syntax

```
isis restart grace-period <1-65535>
no isis restart grace-period
```

Parameters

<1-65535>	Grace period in seconds.

Default

By default, ISIS uses 65535 for the period value, and the value is applied to both level-1 and level-2.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables and then disables a restart grace period at one second.

```
#configure terminal
(config)#isis restart grace-period 1

(config)#no isis restart grace-period
```

isis restart-hello-interval

Use this command to configure the T1 timer, interval of ISIS Hello packet with restart TLV.

Use the no parameter to use the default value.

Command Syntax

```
isis restart-hello-interval <1-65535> (level-1|level-2|)
no isis restart-hello-interval <1-65535> (level-1|level-2|)
no isis restart-hello-interval (level-1|level-2|)
```

Parameters

`<1-65535>`	Specify the number of seconds in the interval.
`level-1`	Specify the hello-interval for level-1 IIHs.
`level-2`	Specify the hello-interval for level-1 IIHs.

Default

By default, ISIS uses 3 seconds for the hello value, and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables a restart hello interval at 123 seconds for a level 1 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#isis restart-hello-interval 123 level-1

(config-if)#no isis restart-hello-interval 123 level-1
```

isis restart helper

Use this command to configure the router's helper mode capability.

Use the no parameter to disable the helper mode for this router.

Command Syntax

```
isis restart helper
no isis restart helper
```

Parameters

None

Default

By default, most routers are not a restart helper router.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables ISIS restart helper.

```
#configure terminal
(config)#isis restart helper

(config)#no isis restart helper
```

isis restart suppress-adjacency

Use this command to enable ISIS to request that its adjacency be suppressed after the ISIS daemon process starts or restarts until the Link State Packet Database (LSPDB) synchronizes.

Use the no parameter to disable suppress-adjacency.

Command Syntax

```
isis restart suppress-adjacency
no isis restart suppress-adjacency
```

Parameters

None

Default

By default, ISIS does not request that its adjacency be suppressed after the ISIS daemon process starts or restarts.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables ISIS restart suppress adjacency.

```
#configure terminal
(config)#isis restart suppress-adjacency

(config)#no isis restart suppress-adjacency
```

restart isis graceful

Use this command to restart the ISIS router.

Command Syntax

```
restart isis graceful (grace-period <1-65535>|)
```

Parameters

<1-65535>	Grace period in seconds.

Default

By default, the ISIS router is not restarted gracefully. Default grace-period is 65535 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#restart isis graceful grace-period 60
```

restart-timer

Use this command to restart the ISIS T2 timer. When a node comes up after graceful restart, within this time, the LSPDB sync should be completed.

Use the no parameter with this command to negate this command.

Command Syntax

```
restart-timer <5-65535> (level-1|level-1-2|level-2|)
no restart-timer (level-1|level-1-2|level-2|)
no restart-timer <5-65535> (level-1|level-1-2|level-2|)
```

Parameters

<5-65535>	Restart time in seconds
level-1	Restart is only for Level-1.
level-1-2	Restart is for both Level-1 and Level-2.
level-2	Restart is only for Level-2.

Default

The default value is 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables the restart timer at 555 seconds for a level 2 interface.

```
#configure terminal
(config)#router isis bb
(config-router)#restart-timer 555 level-2

(config)#router isis bb
(config-router)#no restart-timer 555 level-2
```

CHAPTER 3 IS-IS Show Commands

This chapter provides describes the IS-IS show commands:

show clns is-neighbors

Use this command to display IS neighbor adjacencies.

Command Syntax

```
show clns is-neighbors (detail|)
show clns WORD is-neighbors (detail|)
show clns is-neighbors IFNAME (detail|)
show clns WORD is-neighbors IFNAME (detail|)
```

Parameters

`detail`	Detailed information.
`WORD`	Information for a single IS-IS area.
`IFNAME`	Information for a single interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show clns is-neighbors detail
Tag abc: VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0003 eth1        Up     L1   64        0000.0000.0003.01
L1 Adjacency ID: 1
L2 Adjacency ID: 2
Uptime: 00:12:31
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 3-9 explains the fields in the output.

Table 3-9: show clns is-neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

Table 3-9: show clns is-neighbors output (Continued)

Field	Description
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: IS is considered reachable
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Priority	IS-IS priority that the respective neighbor is advertising. The highest priority neighbor is elected the designated IS-IS router for the interface.
Circuit Id	Number that the router uses to uniquely identify its IS-IS interface. When the interface is attached to a broadcast network, the Circuit ID is concatenated with System ID of the designated router for the interface.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show clns neighbors

Use this command to display ES and IS neighbor adjacencies.

Command Syntax

```
show clns neighbors (detail|)
show clns WORD neighbors (detail|)
show clns neighbors IFNAME (detail|)
show clns WORD neighbors IFNAME (detail|)
```

Parameters

`detail`	Detailed information for all interfaces.
`WORD`	Information for a single IS-IS area.
`IFNAME`	Information for a single interface.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show clns neighbors detail

Tag abc: VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth1        0800.277b.411d  Up     6         L1   IS-IS
L1 Adjacency ID: 1
L2 Adjacency ID: 2
Uptime: 00:15:58
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 3-10 explains the fields in the output.

Table 3-10: show clns neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

Table 3-10: show clns neighbors output (Continued)

Field	Description
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the next-hop.
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: ES or IS is considered reachable
Holdtime	Number of seconds before this adjacency entry times out.
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Protocol	Protocol through which the adjacency was learned.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Topology	IPv4 and/or IPv6.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show debugging isis

Use this command to display the status of the debugging of the ISIS system.

Command Syntax

```
show debugging isis
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging isis
IS-IS debugging status:
IS-IS Interface FSM debugging is on
IS-IS Neighbor FSM debugging is on
IS-IS events debugging is on
IS-IS PDU debugging is on
IS-IS lsp debugging is on
IS-IS spf debugging is on
IS-IS NSM debugging is on
IS-IS Check-sum debugging is on
IS-IS Authentication debugging is on
IS-IS Protocol-error debugging is on
IS-IS Local Updates debugging is on
IS-IS Hello debugging is on
IS-IS BFD debugging is on
IS-IS MPLS debugging is on
IS-IS RIB debugging is on
#
```

show ip isis igp-shortcut-lsp

Use this command to display IS-IS shortcut MPLS label-switched paths (LSPs).

Command Syntax

```
show ip isis (WORD|) igp-shortcut-lsp
```

Parameters

WORD	Information for a single IS-IS area.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis igp-shortcut-lsp
#
```

Table 3-11 explains the fields in the output.

Table 3-11: show ip isis igp-shortcut-lsp output

Field	Description
Tunnel-endpoint	Tunnel endpoint address.
Tunnel-id	Tunnel identifier.
Tunnel-metric	Tunnel metric.
active/inactive	Whether the tunnel is active or inactive.

show ip isis route

Use this command to display IS-IS routing table for IPv4.

Command Syntax

```
show ip isis (WORD|) route
```

Parameters

WORD	Information for a single IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
Tag xyz: VRF : default
          Destination         Metric      Next-Hop            Interface      Tag
L1        10.10.10.0/24       20          11.11.11.1          eth1           0
C         11.11.11.0/24       10          –                   eth1           0
#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 3-12 shows these codes.

Table 3-12 explains the fields in the output.

Table 3-12: route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.
L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 3-12: route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 3-13 shows the route entry fields.

Table 3-13: route entry fields

Field	Description
Code	As explained in Table 3-12.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address of the remote network.
Metric	ISIS metric used for SPF calculation (1-63). When a route is imported into the IS-IS network without a specified metric, IS-IS uses 10 for the metric value and the value is applied to both level-1 and level-2.
Next-Hop	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Interface	Interface used to get to the next-hop address for this route.
Tag	Name that identifies the IS-IS area.

show ip isis route igp-shortcut

Use this command to display the IS-IS IGP shortcut routing table.

Command Syntax

```
show ip isis (WORD|) route igp-shortcut
```

Parameters

WORD	Information for an IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis new_isis route igp-shortcut
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric

Tag aa: VRF : default
     Destination         Metric      Tunnel-ID         Tunnel-End-Point
#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 3-14 shows these codes.

Table 3-14: Route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.
L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 3-14: Route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 3-15 shows the route entry fields.

Table 3-15: Route entry fields

Field	Description
Code	As explained in Table 3-12.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address.
Metric	Tunnel metric.
Tunnel-ID	Tunnel identifier.
Tunnel-End-Point	Tunnel endpoint address.

show ip protocols

Use this command to display IP process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols isis
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip protocols
Routing Protocol is "isis 1 "
Redistributing:
Area Address(es): 52
Distance : (default is 115)
#
```

Table 3-16 explains the output fields.

Table 3-16: show ip protocols output

Field	Description
Routing Protocol	“isis” and the name that identifies the IS-IS area.
Redistributing	Protocols being redistributed (such as RIP, OSPF, or BGP), including metric, metric type (internal or external), and route map.
redistribute isis	Whether redistributing IS-IS level-1 into level-2 and vice versa.
Area Address	Network address of the areas into which the routing process is injecting routes.
Distance: (default is 115)	Administrative distance.

show ip route fast-reroute

Use this command to display Loop Free Alternate Fast Reroute (LFA FRR) routes.

Command Syntax

```
show ip route fast-reroute
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
* - candidate default

IP Route Table for VRF "default"
i L140.40.40.0/24 [115/10] via 10.10.10.142, eth1, 00:00:50
                           [FRR-NH] via 30.30.30.144, eth3

i L150.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:00:50
                           [FRR-NH] via 10.10.10.142, eth1

i L160.60.60.0/24 [115/15] via 10.10.10.142, eth1, 00:00:50
                           [FRR-NH] via 20.20.20.143, eth2
```

show ip isis route fast-reroute

Use this command to display Loop Free Alternate Fast Reroute (LFA FRR) route information and interfaces on which LFA FRR is disabled.

Command Syntax

```
show ip isis (WORD|) route fast-reroute
```

Parameters

`WORD` Routing area tag.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p - stale info
* - candidate default

IP Route Table for VRF "default"
i L140.40.40.0/24 [115/10] via 10.10.10.142, eth1, 00:00:50
                          [FRR-NH] via 30.30.30.144, eth3

i L150.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:00:50
                          [FRR-NH] via 10.10.10.142, eth1

i L160.60.60.0/24 [115/15] via 10.10.10.142, eth1, 00:00:50
                          [FRR-NH] via 20.20.20.143, eth2
```

show ip isis lfa-config

Use this command to display the Loop Free Alternate Fast Reroute (LFA FRR) tie-break preferences for protection types and the termination hold-on timer.

Command Syntax

```
show ip isis (WORD|) lfa-config (level-1|level-2)
```

Parameters

`WORD` Routing area tag.

`level-1` Level 1 only.

`level-2` Level 2 only

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip isis lfa-config level-1

TIE-Breaker           Preference values
-----------------------------------------------
Primary Path:                 20
Link Protecting:              30
Node Protecting:              60
Broadcast Interface Disjoint: 70
Secondary Path:                0
Downstream Path:               0
```

Termination Hold On Interval : 1000 ms

show isis counter

Use this command to display the MIB variables used to construct routing tables for IP networks for IS-IS as defined in RFC 4444.

Command Syntax

```
show isis counter
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis counter
Tag abc: VRF : default
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 7
isisSysStatPRCRuns: 0

IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 3
isisSysStatPRCRuns: 0
#
```

show isis database

Use this command to display link-state database (LSDB) database information. The LSDB is the core of IS-IS routing. All link-state information advertised by neighbors in the same area is stored in the LSDB.

Command Syntax

```
show isis database
show isis database (detail|verbose)
show isis database (detail|verbose) WORD
show isis database (detail|verbose) WORD (l1|l2|level-1|level-2)
show isis database (detail|verbose) (l1|l2|level-1|level-2)
show isis database (detail|verbose) (l1|l2|level-1|level-2) WORD
show isis database WORD
show isis database WORD (l1|l2|level-1|level-2)
show isis database WORD (l1|l2|level-1|level-2) (detail|verbose)
show isis database WORD (detail|verbose)
show isis database WORD (detail|verbose) (l1|l2|level-1|level-2)
show isis database (l1|l2|level-1|level-2)
show isis database (l1|l2|level-1|level-2) (detail|verbose)
show isis database (l1|l2|level-1|level-2) (detail|verbose) WORD
show isis database (l1|l2|level-1|level-2) WORD
show isis database (l1|l2|level-1|level-2) WORD (detail|verbose)
```

Parameters

`detail`	Detailed information.
`verbose`	Verbose information.
`WORD`	Link-state packet (LSP) identifier in the form of XXXX.XXXX.XXXX.XX-XX.
`l1`	IS-IS level-1.
`l2`	IS-IS level-2.
`level-1`	IS-IS level-1.
`level-2`	IS-IS level-2.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis database detail
Area bb:
IS-IS Level-1 Link State Database:
```

```
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
000F.0000.0001.00-00* 0x00000007   0xE15E        1188              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  IP Address:   10.10.12.97
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02
000F.0000.0001.02-00* 0x00000003   0x3C66        1026              1/0/0
  Metric:  0         IS 000F.0000.0001.00
  Metric:  0         IS 000F.0000.0002.00
000F.0000.0002.00-00  0x00000003   0x8C4B        1025              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  Hostname:     isisd@redhat
  IP Address:   10.10.12.94
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02
#
```

Table 3-17 explains the output fields.

Table 3-17: show isis database output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS Level-n Link State Database	Each IS-IS level has a section with Link-State Packet (LSP) information.
LSPID	Link-state packet identifier in the form of XXXX.XXXX.XXXX.XX-XX. The first six octets (“XXXX.XXXX.XXXX”) are the system identifier of the router that originated the LSP. The next octet is the pseudonode identifier: • When this octet is nonzero, the LSP describes links from a designated router (pseudonode) that creates and floods an LSP that describes all systems attached to the network. This mechanism is similar to a router link-state advertisement (LSA) in OSPF. • When this octet is zero, the LSP is from a nonpseudonode which describes the state of the originating router. The last octet is the LSP number. If the value is 0x00, the entire LSP was carried in one LSP. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments and each fragment has a different LSP number. An asterisk (*) means the LSP originated on the system where the command was given.
LSP Seq Num	LSP sequence number.
LSP Checksum	LSP checksum.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero means the LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	Attached bit. A Level-2 IS indicates its attachment to other areas by setting its attached bit in its Level-1 LSP 0. In other words, this is only set for inter-area routes. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the attach bit to find the closest Level-2 router. They will point a default route to the closest Level-2 router.

Table 3-17: show isis database output

Field	Description
P	Partition repair. A Level-1 area can become partitioned; this bit means the partition can be repaired via use of Level-2 routes.
OL	Overload bit. Determines whether the IS is congested. When the overload-bit is set in an LSP, other routers will not use this router as a transit router during SPF calculation. Only packets for destinations directly connected to the overloaded router will be sent to this router.

This command also displays information about the IS-IS TLVs in Table 3-18 if present in an LSP. For more about the TLV information, search for “IS-IS TLV Codepoints” on the Interne, check ISO/IEC 10589:2002(E), or other standard mentioned in Table 3-18.

Table 3-18: IS-IS TLV Codepoints

IS-IS TLV Codepoint	Description	Standard
1	Area Addresses	ISO 10589
2	IIS Neighbors	ISO 10589
3	ES Neighbors	ISO 10589
10	Authentication	ISO 10589, RFC 6233
22	Extended IS reachability	RFC 5305
128	IP internal reachability	RFC 1195, RFC 5302
129	Protocols supported	RFC 1195
130	IP external reachability	RFC 1195, RFC 5302
132	IP interface address	RFC 1195
134	Traffic engineering router ID	RFC 5305
135	Extended IP reachability	RFC 5305
137	Host name	RFC 5301, RFC 6233
222	Multi IS reachability	RFC 5120
229	Multi topology	RFC 5120
232	IPv6 interface address	RFC 5308
235	Multi IPv4 reachability	RFC 5120
236	IPv6 reachability	RFC 5308
237	Multi IPv6 reachability	RFC 5120

show isis interface

Use this command to display detailed interface information.

Command Syntax

```
show isis interface
show isis interface IFNAME
show isis interface counter
```

Parameters

IFNAME	Interface name.
counter	Interface counters.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>show isis interface
eth2 is up, line protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000004
Local SNPA: 0800.2731.a9a0
IP interface address:
10.10.10.1/24
IPv6 interface address:
fe80::a00:27ff:fe31:a9a0/64
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
Number of active level-2 adjacencies: 0
Level-2 LSP MTU: 1492
Next IS-IS LAN Level-2 Hello in 9 seconds
eth1 is up, line protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000003
Local SNPA: 0800.2714.e7f8
IP interface address:
11.11.11.1/24
IPv6 interface address:
fe80::a00:27ff:fe14:e7f8/64
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
Number of active level-1 adjacencies: 1
Level-1 LSP MTU: 1492
```

```
    Next IS-IS LAN Level-1 Hello in 5 seconds

    >show isis interface eth1
    eth1 is up, line protocol is up
    Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000003
    Local SNPA: 0800.27e3.0e64
    IP interface address:
    30.0.0.1/24
    IPv6 interface address:
    fe80::a00:27ff:fee3:e64/64
    LDP-ISIS Sync Configured
    Holddown timer = 100 seconds, Remaining time = 90 seconds
    Level-1 Metric: 63/16777214, Priority: 64, Circuit ID: 0000.0000.0001.02
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 1 seconds
```

Table 3-19 explains the output fields.

Table 3-19: show isis interface

Field	Description
IFNAME is up, line protocol is up/down	Whether the interface is up or down
Routing Protocol	“IS-IS” and the name that identifies the IS-IS instance.
Network Type	• Broadcast • Point-to-Point • Loopback
Circuit Type	Whether the interface is configured for: • Local routing: level-1 • Area routing: level 2 • Local and area routing: level-1-2
Local circuit ID	Local circuit identifier assigned when interface is created. Each IS-IS interface is assigned a circuit identifier to identify the interface within the link-state database. If the interface is attached to a multiaccess network, the circuit ID is concatenated with the system ID of the designated IS. This is called the pseudonode ID.
Extended Local circuit ID	Interface index.
Local SNPA	SubNetwork Point of Attachment: for broadcast networks, MAC address.
IP interface address	IPv4 addresses assigned to IS-IS interface.
IPv6 interface address	IPv6 addresses assigned to IS-IS interface.
LDP-ISIS Sync Configured	LDP IS-IS synchronization is enabled.

Table 3-19: show isis interface (Continued)

Field	Description
Holddown timer	Delay for notifications of LDP convergence to IS-IS
Remaining time	Remaining LDP convergence hold time in seconds.
Holddown timer not configured	The LDP convergence holddown timer has not been set.
Level-1 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.
Number of active level-1 adjacencies	Number of adjacencies formed with a neighboring router.
Level-1 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Level-2 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.
Number of active level-2 adjacencies	Number of adjacencies formed with a neighboring router.
Level-2 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Next IS-IS LAN Level-1 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS LAN Level-2 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS Hello in	For point-to-point networks, when the next IS hello will be sent on this interface.
Bandwidth	Traffic engineering: interface bandwidth.
Maximum reservable bandwidth	Traffic engineering: maximum reservable interface bandwidth.
Available bandwidth at priority	Traffic engineering: available interface bandwidth at priority.
Bidirectional Forwarding Detection is disabled/enabled/ configured	BFD state

show isis tag database

Use this command to display detailed link-state database information for an IS-IS routing area.

Command Syntax

```
show isis WORD database
show isis WORD database (detail|verbose)
show isis WORD database (detail|verbose) WORD
show isis WORD database (detail|verbose) WORD (l1|l2|level-1|level-2)
show isis WORD database (detail|verbose) (l1|l2|level-1|level-2)
show isis WORD database (detail|verbose) (l1|l2|level-1|level-2) WORD
show isis WORD database WORD
show isis WORD database WORD (l1|l2|level-1|level-2)
show isis WORD database WORD (l1|l2|level-1|level-2) (detail|verbose)
show isis WORD database WORD (detail|verbose)
show isis WORD database WORD (detail|verbose) (l1|l2|level-1|level-2)
show isis WORD database (l1|l2|level-1|level-2)
show isis WORD database (l1|l2|level-1|level-2) (detail|verbose)
show isis WORD database (l1|l2|level-1|level-2) (detail|verbose) WORD
show isis WORD database (l1|l2|level-1|level-2) WORD (detail|verbose)
show isis WORD database (l1|l2|level-1|level-2) WORD
```

Parameters

`WORD`	Name that identifies the IS-IS area.
`detail`	Detailed database information.
`verbose`	Verbose database information.
`WORD`	Link-state packet (LSP) identifier in the form of XXXX.XXXX.XXXX.XX-XX.
`l1`	IS-IS level-1 link state database.
`l2`	IS-IS level-2 link state database.
`level-1`	IS-IS level-1 link state database.
`level-2`	IS-IS level-2 link state database.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh isis abc database verbose
Tag abc: VRF : default
```

```
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000008   0xA076        1018              0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.1
Metric: 10 IS 0000.0000.0003.01
Metric: 10 IP 11.11.11.0 255.255.255.0
Metric: 10 IP 10.10.10.0 255.255.255.0
0000.0000.0003.00-00 0x00000007 0x1CB0 1029 0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.2
Metric: 10 IS 0000.0000.0003.01
Metric: 10 IP 11.11.11.0 255.255.255.0
0000.0000.0003.01-00 0x00000005 0x0ACB 1000 0/0/0
Metric: 0 IS 0000.0000.0003.00
Metric: 0 IS 0000.0000.0001.00

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000007   0x7243        988               0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.1
Metric: 10 IP 11.11.11.0 255.255.255.0
Metric: 10 IP 10.10.10.0 255.255.255.0
```

See Table 3-17 and Table 3-18 for an explanation of the output of this command.

show isis topology

Use this command to display paths to Intermediate Systems.

Command Syntax

```
show isis topology (l1|l2|level-1|level-2|)
show isis WORD topology (l1|l2|level-1|level-2|)
```

Parameters

WORD	Display information for specified instance.
l1	Display the path to all level-1 routers in the area.
l2	Display the path to all level-2 routers in the domain.
level-1	Display the path to all level-1 routers in the area.
level-2	Display the path to all level-2 routers in the domain.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis topology

Tag abc: VRF : default
IS-IS paths to level-1 routers
System Id           Metric     Next-Hop            Interface   SNPA
000F.0000.0001      --
000F.0000.0002      10         000F.0000.0002      eth2        0006.5B0E.D27D

IS-IS paths to level-2 routers
System Id           Metric     Next-Hop            Interface   SNPA
0000.0000.0001      10         0000.0000.0001      eth2        0000.0CFA.F002
```

Table 3-20 explains the output fields.

Table 3-20: show isis topology output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS paths to level-n routers	Each IS-IS level has a section with topology information.
System Id	Uniquely identifies a system within an area.
Metric	ISIS metric used for SPF calculation (1-63).

Table 3-20: show isis topology output

Field	Description
Next-Hop	This route is available through the next hop router located at this IP address.
Interface	Interface from which the system was learned.
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the device.

show running-config interface isis

Use this command to display the ISIS interface configuration.

Command Syntax

```
show running-config interface IFNAME isis
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth0 isis
!
interface eth0
 isis tag 500 level-1
!
```

show running-config router isis

Use this command to display the ISIS router configuration.

Command Syntax

```
show running-config router isis
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config-router)#show running-config router isis
!
router isis
!
```

Unicast Routing Information Base Command Reference

Contents

This document contains this chapter:

CHAPTER 1 Unicast RIB Commands

This chapter describes the following unicast RIB commands:

clear ip route kernel

Use this command to clear stale IPv4 routes from the RIB (Routing Information Base) and FIB (Forwarding Information Base).

Command Syntax

```
clear ip route kernel
clear ip kernel route
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route kernel
```

clear ip route

Use this command to clear an all IPv4 routes or any specific prefix routes.

Command Syntax

```
clear ip route (*|A.B.C.D/M)
```

Parameters

*	Clears all routes
A.B.C.D/M	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route *
#clear ip route 1.1.1.0/24
```

clear ip route vrf NAME

Use this command to clear all IPv4 VRF route or any specific prefix VRF route of any particular VRF name.

Command Syntax

```
clear ip route vrf NAME (*|A.B.C.D/M)
```

Parameters

NAME	VPN Routing or Forwarding instance name
*	Clears all routes
A.B.C.D/M	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route vrf myVRF *
```

debug rib

Use this command to debug the `ribd` process.

Use the `no` form of this command or the `undebug` command to stop debugging.

Command Syntax

```
debug rib (all|)
debug rib events
debug rib packet (recv|send|) (detail|)
debug rib nsm
debug rib bfd
debug rib monitor
debug ip routing (add-route|delete-route|mod-route|
no debug all
no debug rib (all|)
no debug all rib
no debug rib events
no debug rib packet (recv|send|) (detail|)
no debug rib nsm
no debug rib bfd
no debug rib monitor
no debug ip routing (add-route|delete-route|mod-route|)
undebug all
undebug rib (all|)
undebug all rib
undebug rib events
undebug rib packet (recv|send|) (detail|)
undebug rib nsm
undebug rib bfd
```

Parameters

`all`	All debugging functions
`events`	Events
`packet`	Packet events
`recv`	Received packets
`send`	Sent packets
`detail`	Detailed information
`nsm`	NSM events
`monitor`	Monitoring the kernel Netlink messages

`bfd`	BFD (Bidirectional Forwarding Detection) events
`ip routing`	IPv4 routing events
`add-route`	Add route events
`delete-route`	Delete route events
`mod-route`	Modify route events

Disabled

By default, debug command is disabled.

Command Mode

Privileged Exec mod

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug rib all
```

description

Use this command to assign a description to a Virtual Router instance.

Use the no parameter to remove a description.

Command Syntax

```
description LINE
no description
```

Parameters

LINE	Virtual Router description maximum 80 characters

Disabled

By default, description command is disabled

Command Mode

VR mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#description VR1 has been created for CLI testing
(config-vr)#exit

(config)#virtual-router VR1
(config-vr)#no description
(config-vr)#exit
```

fib retain

Use this command to set the retention time for stale routes in the Forwarding Information Base (FIB) when `ribd` restarts. The `ribd` process reads the FIB and treats previously self-installed routes as stale.

You can display stale routes by running the `show ip route database` command. All routes preceded by the symbol p are stale routes. When protocol modules restart, `ribd` overrides these stale routes with routes updated by the protocol modules.

Table 1-21 show the behavior of routes when `ribd` stops.

Table 1-21: FIB retention

Command	Behavior
`fib retain`	Does not clear routes from the FIB and retains stale routes for 60 seconds when restarted.
`fib retain forever`	Does not clear routes and retains stale routes forever.
`fib retain time <1-65535>`	Does not clear routes and retains stale routes for the specified seconds.
`no fib retain` (default)	Cleans up routes in the FIB, but retains stale routes for 60 seconds when restarted.

You can remove stale routes at any time with the clear ip route kernel command.

Use the `no` form of this command to revert to default; that is, do not retain routes in the FIB when `ribd` stops.

Command Syntax

```
fib retain (forever|time <1-65535>|)
no fib retain (forever|time <1-65535>|)
```

Parameters

`forever`	Retain FIB forever
`time`	Retain FIB for a time after `ribd` restarts
`<1-65535>`	Retention time in seconds; if you omit this value, the default is 60 seconds

Default

Routes are cleared from the FIB when `ribd` stops. However, when `ribd` restarts, stale routes are retained for 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#fib retain time 180
```

ip route

Use this command to create an IPv4 static route.

Use the no form of this command to delete a static route.

Command Syntax

```
ip route A.B.C.D/M (A.B.C.D|IFNAME)
ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME)
ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description WORD}
ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description
  WORD}
ip route A.B.C.D/M IFNAME A.B.C.D
ip route vrf NAME A.B.C.D/M IFNAME
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME global
ip route vrf NAME A.B.C.D/M IFNAME {<1-255>|tag <0-4294967295>|description WORD}
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-4294967295>|description
  WORD}
no ip route A.B.C.D/M (A.B.C.D|IFNAME|)
no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME)
no ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description WORD}
no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description
  WORD}
no ip route vrf NAME A.B.C.D/M IFNAME
no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME
no ip route vrf NAME A.B.C.D/M IFNAME {<1-225>|tag <0-4294967295>|description WORD}
no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-
  4294967295>|description WORD}
```

Parameters

A.B.C.D/M	Subnet: IP destination prefix and a mask length
A.B.C.D A.B.C.D	Subnet: IP destination address and mask
A.B.C.D	Gateway nexthop IPv4 address
IFNAME	Gateway nexthop interface name
global	Global table lookup (to support inter-VRF static route leaking)
<1-255>	Administrative distance
description	Description of the static route maximum 80 character. For larger description use hypen (-) or underscore (_), as space is not supported.
tag	Tag used as a “match” value to control redistribution via route maps

<0-4294967295>	
	Tag value
vrf	VRF (Virtual Routing and Forwarding) instance
NAME	VRF name

Default

By default, no static IPv4 route is configured

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and was updated in OcNOS version 1.3.4 and OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ip route 192.168.3.0 255.255.255.0 2.2.2.2 128
(config)#ip route 1.1.1.0/24 eth0 32
(config)#ip route vrf new 1.1.1.1/1 1.1.1.1 eth1 description new tag 1
```

This example creates static routes in default VRF with the nexthops belonging to the Non default VRF.

```
(config)#ip route 20.1.1.0/24 ce0 30.1.1.3
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
- candidate default
IP Route Table for VRF "default"
C 4.4.4.4/32 is directly connected, lo, 05:05:04
O 5.5.5.5/32 [110/2] via 40.1.1.5, xe0, 05:03:40
S v 20.1.1.0/24 [1/0] via 30.1.1.3, ce0, 00:00:24
C 40.1.1.0/24 is directly connected, xe0, 05:05:04
C 70.1.1.0/24 is directly connected, xe2, 05:05:04
O 80.1.1.0/24 [110/2] via 70.1.1.1, xe2, 02:54:01
S 90.1.1.0/24 [1/0] is directly connected, xe2, 00:02:40
C 127.0.0.0/8 is directly connected, lo, 05:16:21Gateway of last
resort is not set
```

This example creates VRF static routes with the nexthops belonging to the default VRF. The nexthop gateway address can be the IFNAME network address or any other IP address reachable via IFNAME.

```
#show ip route vrf
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
```

```
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.12.19.0/24 is directly connected, eth0, 4d23h06m
C     11.1.1.0/24 is directly connected, eth4, 4d23h01m
C     13.13.13.0/31 is directly connected, eth3, 4d23h06m
C     50.5.5.0/24 is directly connected, eth3, 4d23h06m
C     100.100.100.0/24 is directly connected, lo, 4d23h06m
O     101.1.1.1/32 [110/11] via 11.1.1.2, eth4, 19:20:39
C     127.0.0.0/8 is directly connected, lo, 4d23h06m
Gateway of last resort is not set

(config)#ip route vrf vrf1 201.201.201.201/32 11.1.1.11 eth4 global
(config)#ip route vrf vrf1 202.202.202.202/32 101.1.1.1 eth4 global

#show ip route vrf vrf1 static
IP Route Table for VRF "vrf1"
S    v201.201.201.201/32 [1/0] via 11.1.1.11, eth4, 00:00:44
S    v202.202.202.202/32 [1/0] via 101.1.1.1, eth4 (recursive via 11.1.1.2), 00:00:17
Gateway of last resort is not set
```

ip vrf

This command creates a VRF (Virtual Routing and Forwarding) RIB (Routing Information Base), assigns a VRF identifier, and switches to VRF mode.

Use the no parameter with command to remove a VRF RIB.

Command Syntax

```
ip vrf WORD
no ip vrf WORD
```

Parameter

WORD	VRF identifier

Default

By Default, ip vrf is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#
```

ipv6 route

Use this command to create an IPv6 static route.

Use the no form of this command to delete a static route

Note: IPv6 static route with Interface name alone as gateway next-hop is not supported.

Command Syntax

```
ipv6 route X:X::X:X/M (X:X::X:X|IFNAME) {<1-255>}
ipv6 route X:X::X:X/M X:X::X:X IFNAME {<1-255>}
ipv6 route vrf NAME X:X::X:X/M (X:X::X:X|IFNAME)
ipv6 route vrf NAME X:X::X:X/M X:X::X:X IFNAME
no ipv6 route X:X::X:X/M (X:X::X:X|IFNAME) {<1-255>}
no ipv6 route X:X::X:X/M X:X::X:X IFNAME {<1-255>}
no ipv6 route vrf NAME X:X::X:X/M (X:X::X:X|IFNAME)
no ipv6 route vrf NAME X:X::X:X/M X:X::X:X IFNAME
```

Parameter

`X:X::X:X/M`	Subnet: IPv6 destination prefix and a mask length
`X:X::X:X`	Gateway nexthop IPv6 address
`IFNAME`	Gateway nexthop interface name
`<1-255>`	Administrative distance
`vrf`	VRF (Virtual Routing and Forwarding) instance
`NAME`	VRF name

Default

By default, no static IPv6 route is configured

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 route 1234::/64 1000::1 128
(config)#ipv6 route 1235::/64 eth1 32
(config)#ipv6 route vrf vrf3 1236::/64 eth3
(config)#end
#show ipv6 route vrf all
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
IA - OSPF inter area, E1 - OSPF external type 1,
E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
```

```
N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 23:35:55
C      2::2/128 via ::, lo, 23:35:55
C      1000::/64 via ::, eth1, 00:07:45
S      1234::/64 [128/0] via 1000::1, eth1, 00:07:04
S      1235::/64 [32/0] via ::, eth1, 00:06:38
C      6000::/64 via ::, eth1, 23:35:55
C      7000::/64 via ::, eth7, 23:35:55
C      fe80::/64 via ::, eth7, 23:35:55
IP Route Table for VRF "management"
IP Route Table for VRF "vrf3"
S      1236::/64 [1/0] via ::, eth3, 00:00:13
C      3000::/64 via ::, eth3, 00:07:55
C      fe80::/64 via ::, eth3, 00:08:05

#show ipv6 route vrf all static
IP Route Table for VRF "default"
S      1234::/64 [128/0] via 1000::1, eth1, 00:15:28
S      1235::/64 [32/0] via ::, eth1, 00:15:02
IP Route Table for VRF "management"
IP Route Table for VRF "vrf3"
S      1236::/64 [1/0] via ::, eth3, 00:08:37
```

maximum-paths

Use this command to set the maximum number of paths to install in the FIB (Forwarding Information Base) for the ECMP (Equal-Cost MultiPath) feature.

Use the no parameter with this command to revert to default.

Note: If you change the number of paths from the default (8), you must save the running configuration and perform a reboot.

Command Syntax

```
maximum-paths <1-64>
no maximum-paths
```

Parameter

<1-64>	Maximum number of paths to install in the FIB

Default

By default, the maximum number of paths is 8.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#maximum-paths 5
```

max-fib-routes

Use this command to set the maximum number of FIB (Forwarding Information Base) routes including kernel, connected, and static routes.

Use the no parameter to remove this configuration.

Command Syntax

```
max-fib-routes <1-16384>
no max-fib-routes
```

Parameters

<1-16384>	Maximum number of FIB routes, including kernel, connected, and static routes

Default

By default, no FIB routes configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#max-fib-routes 12345

(config)#no max-fib-routes
```

max-static-routes

Use this command to set the maximum number of static routes.

Use the no parameter to disable this command.

Command Syntax

```
max-static-routes <1-4294967294>
no max-static-routes
```

Parameters

`<1-4294967294>` Maximum number of static routes

Default

By default, max static routes value is 4294967294

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#max-static-routes 123

(config)#no max-static-routes
```

show debugging rib

Use this command to display debug settings.

Command Syntax

```
show debugging rib
```

Parameters

None

Command Mode

Privileged Exec Mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging rib
```

snmp restart rib

Use this command to restart SNMP in Routing Information Base (RIB)

Command Syntax

```
snmp restart rib
```

Parameters

None

Default

By default, snmp restart command is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#snmp restart rib
```

Two-Way Active Measurement Protocol Command Reference

Contents

This document contains these chapters and appendix:

CHAPTER 1 TWAMP Commands

This chapter describes the commands used to manage the Two-Way Active Measurement Protocol (TWAMP), including TWAMP light control, TWAMP light reflector, and TWAMP light sender.

twamp-light control

Use this command to initialize the TWAMP light Control or Sender Session.

Use the no form of this command to un-initialize and to remove the configured TWAMP light control configurations.

Command Syntax

```
twamp-light control
no twamp-light control
```

Parameters

NA

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#twamp-light control
```

control-admin-state

Use this command to enable or disable the TWAMP control sessions.

Command Syntax

```
control-admin-state (enable | disable)
```

Parameters

`enable`	Enable the TWAMP control session.
`disable`	Disable the TWAMP control session.

Default

disable

Command Mode

TWAMP light control mode (config-twamp-light-ctrl)

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
(config)#twamp-light control
(config-twamp-light-ctrl)#control-admin-state enable
```

test-session-name

Use this command to configure the TWAMP test sessions.

Use the no form of this command to un-configure or remove the configured TWAMP test sessions.

Command Syntax

```
test-session-name WORD sender-ip (X:X::X:X | A.B.C.D) (sender-port <1025-65535>|)
  (reflector-ip (X:X::X:X | A.B.C.D)) (reflector-port <1025-65535>|)
no test-session-name WORD
```

Parameters

WORD	TWAMP test session name.
X:X::X:X	TWAMP Sender or Reflector IP address in IPv6 format.
A.B.C.D	TWAMP Sender or Reflector IP address in IPv4 format.
<1025-65535>	TWAMP Sender or Reflector UDP port number.

Note: sender-port and reflector-port are optional parameters

Default

862 for sender-port and reflector-port

Command Mode

TWAMP light control mode (config-twamp-light-ctrl)

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

To Configure

```
(config)#twamp-light control
(config-twamp-light-ctrl)# test-session-name s1 sender-ip 10.0.0.1 sender-port
1234 reflector-ip 10.0.0.1 reflector-port 1234
```

To un-configure

```
(config)#twamp-light control
(config-twamp-light-ctrl)# no test-session-name s1
```

twamp-light reflector

Use this command to initialize the TWAMP reflector.

Use the no form of this command to un-initialize and to remove the configured TWAMP light refelctor configurations.

Command Syntax

```
twamp-light reflector
no twamp-light reflector
```

Parameters

NA

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#twamp-light reflector
```

reflector-admin-state

Use this command to enable or disable the TWAMP reflector session.

Command Syntax

```
reflector-admin-state (enable | disable)
```

Parameters

`enable`	Enable the TWAMP reflector session.
`disable`	Disable the TWAMP reflector session.

Default

disable

Command Mode

TWAMP light reflector mode (config-twamp-light-ctrl)

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
(config)#twamp-light reflector
(config-twamp-light-ctrl)#reflector-admin-state enable
```

reflector ip

Use this command to configure the TWAMP light reflector session.

Command Syntax

```
reflector-ip (X:X::X:X | A.B.C.D) (reflector-port <1025-65535>|)
```

Parameters

`X:X::X:X`	TWAMP Reflector IP address in IPv6 format.
`A.B.C.D`	TWAMP Reflector IP address in IPv4 format.
`<1025-65535>`	TWAMP Reflector UDP port number.

Note: reflector-port is optional parameter

Default

862 for reflector-port

Command Mode

TWAMP light reflector mode (config-twamp-light-ctrl)

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
(config)#twamp-light reflector
(config-twamp-light-ref)#reflector-ip 10.0.0.1 reflector-port 1234
```

twamp start-test-session

Use this command to start the TWAMP test session.

Command Syntax

```
twamp start test-session WORD packet-count <1-65535> (interval <500-10000>|)
```

Parameters

WORD	TWAMP test session name.
<1-65535>	Number packed to send for test.
<500-10000>	Interval to send each packet in milliseconds.

Note: interval is optional parameters.

Default

1000 for interval

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#twamp start test-session s1 packet-count 10 interval 500
```

twamp stop-test-session

Use this command to stop the TWAMP test session.

Command Syntax

```
twamp stop test-session WORD
```

Parameters

WORD	TWAMP test session name.

Default

NA

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#twamp stop test-session s1
```

show twamp statistics

Use this command to display TWAMP test session.

Command Syntax

```
show twamp-statistics (WORD|)
```

Parameters

WORD	TWAMP test session name.

Note: WORD is optional parameter

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#show twamp statistics
=======================================
      TWAMP Test-Session Statistics
=======================================
  Test-Session Name        : s1
  Start Time               : 2019 Aug 05 08:40:12
  Elapsed time(milli sec)  : 4004
  Packets Sent             : 4
  Packets Received         : 4
  Packet Loss(%)           : 0.0000
  Round Trip Delay(usec)
      Minimum              : 585
      Maximum              : 2306
      Average              : 1038
  Forward Delay(usec)
      Minimum              : 254
      Maximum              : 318
      Average              : 280
  Reverse Delay(usec)
      Minimum              : 331
      Maximum              : 1988
      Average              : 758
  Round Trip Delay Variation(usec)
      Minimum              : 2306
      Maximum              : 2640
      Average              : 2444
  Forward Delay Variation(usec)
      Minimum              : 318
      Maximum              : 375
      Average              : 345
  Reverse Delay Variation(usec)
      Minimum              : 1988
      Maximum              : 2265
```

```
Average              : 2099
```

Table 1-22: show twamp statistics

Field	Description
Test-Session Name	TWAMP test session name
Start Time	TWAMP test start time
Elapsed time(milli sec)	Time taken to complete the test in milliseconds
Packets Sent	Number of packet sent
Packets Received	Number of packet received
Packet Loss(%)	Packet lost in percentage
Round Trip Delay(usec)	Round trip delay between TWAMP sender and reflector. Displayed Minimum, Maximum and Average round trip delay in micro-seconds
Forward Delay(usec)	Forward delay between TWAMP sender and reflector. Displayed Minimum, Maximum and Average forward delay in micro-seconds
Reverse Delay(usec)	Reverse delay between TWAMP reflector and sender. Displayed Minimum, Maximum and Average reverse delay in micro-seconds
Round Trip Delay Variation(usec)	Round trip delay variation between TWAMP sender and reflector. Displayed Minimum, Maximum and Average round trip delay variation in micro-seconds
Forward Delay Variation(usec)	Forward delay variation between TWAMP sender and reflector. Displayed Minimum, Maximum and Average forward delay variation in micro-seconds
Reverse Delay Variation(usec)	Reverse delay variation between TWAMP reflector and sender. Displayed Minimum, Maximum and Average reverse delay variation in micro-seconds

show running-config twamp

Use this command to display TWAMP running configuration alone.

Command Syntax

```
show running-config twamp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

Reflector:

```
#show running-config twamp
twamp-light reflector
 reflector-admin-state enable
 reflector-ip 10.0.0.1 reflector-port 1234
```

Control or Sender:

```
#show running-config twamp
twamp-light control
 control-admin-state enable
 test-session-name s1 sender-ip 10.0.0.1 sender-port 1234 reflector-ip
10.0.0.1 reflector-port 1234
```

Layer 3 Subinterface Commands

Contents

This document contains these chapters and appendix:

CHAPTER 1 Layer 3 Subinterface Commands

This chapter describes the Layer 3 subinterface commands:

encapsulation

Use this command to configure encapsulation under a subinterface. Using this command, a Layer 3 subinterface can be configured as a port-vlan or stacked vlan. Before configuring the encapsulation on sub-interface, the operating state of the sub-interface is admin down. After configuring the encapsulation, the operating state of the sub-interface becomes up.

Command Syntax

```
encapsulation ((dot1q|dot1ad) VLAN_ID (inner-dot1q VLAN_ID|))
no encapsulation
```

Parameters

`dot1q`	IEEE 802.1Q VLAN-tagged packets
`dot1ad`	IEEE 802.1ad VLAN-tagged packets
`VLAN_ID`	First (outer) VLAN identifier on the subinterface <2-4094>
`inner-dot1q VLAN_ID`	Second (inner 802.1Q) VLAN identifier on the subinterface <2-4094>

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config-if)#interface xe9.1
(config-if)#encapsulation dot1q 10

(config-if)#interface xe9.2
(config-if)#encapsulation dot1q 20 inner-dot1q 20

(config-if)#interface xe9.3
(config-if)#encapsulation dot1ad 30

(config-if)#interface xe9.4
(config-if)#encapsulation dot1ad 40 inner-dot1q 40
```

interface IFNAME.SUBINTERFACE_ID

Use this command to configure a subinterface. A subinterface can only be created on a Layer 3 parent interface. Subinterfaces are supported for raw Ethernet interfaces as well as dynamic/static LAG interfaces. The number of subinterfaces supported is 2000 per parent port and a total of 4000 sub-interfaces per device. This command displays an error when the identifier of the subinterface is out of range.

Use no form of this command to unconfigure a sub-interface.

Command Syntax

```
interface IFNAME.SUBINTERFACE_ID
no interface IFNAME.SUBINTERFACE_ID
```

Parameters

IFNAME	Interface name, such as xe1, po1, or sa1
SUBINTERFACE_ID	Subinterface identifier <1-2000>

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#int xe1.5
(config-if)#exit
(config)#no interface xe1.5

(config)#int po1
(config-if)#exit
(config)#int po1.1
(config-if)#exit
(config)#no interface po1.1

(config)#int sa1
(config-if)#exit
(config)#int sa1.1
(config-if)#exit
(config)#no interface sa1.1
```

show interface IFNAME.SUBINTERFACE_ID

Use this command to display the details of the sub-interface.This command displays the information about the operating status, hardware address, VRF binding details, and input/output counters. This command can display details of the a sub-interface for a dynamic/static LAG as well.

Command Syntax

```
show interface IFNAME.SUBINTERFACE_ID
```

Parameters

IFNAME	Interface name, such as xe1, po1, or sa1
SUBINTERFACE_ID	Subinterface identifier <1-2000>

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show int xe1.1
Interface xe1.1
  Hardware is SUBINTERFACE  Current HW addr: 6cb9.c500.1647
  Physical:6cb9.c500.1647  Logical:(not set)
  Port Mode is Router
  Interface index: 20482049
  Metric 1 mtu 1500
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  inet6 fe80::6eb9:c5ff:fe00:1647/64
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
```

```
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show int sa1.1
Interface sa1.1
  Hardware is SUBINTERFACE  Current HW addr: 6cb9.c500.1647
  Physical:6cb9.c500.1647  Logical:(not set)
  Port Mode is Router
  Interface index: 409602049
  Metric 1 mtu 1500
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  inet6 fe80::6eb9:c5ff:fe00:1647/64
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show int po1.3
Interface po1.3
  Hardware is SUBINTERFACE  Current HW addr: 0030.abf1.0ec8
  Physical:0030.abf1.0ec8  Logical:(not set)
  Port Mode is Router
  Interface index: 204802051
  Metric 1 mtu 1500
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
```

```
DHCP client is disabled.
Last Flapped: Never
Statistics last cleared: Never
inet 23.0.0.2/24 broadcast 23.0.0.255
inet6 fe80::230:abff:fef1:ec8/64
RX
  unicast packets 0 multicast packets 0 broadcast packets 0
  input packets 141805 bytes 9643544
  jumbo packets 0
  undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
  input error 0
  input with dribble 0 input discard 0
  Rx pause 0
TX
  unicast packets 0 multicast packets 0 broadcast packets 0
  output packets 0 bytes 0
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0
```

SECTION 7 Multicast

Multicast Configuration Guide

Contents

This document contains these chapters and appendices:

CHAPTER 1 IGMP Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP).

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers.

Using the information obtained through IGMP, the router maintains a list of multicast group on a per-interface basis. The routers that receive these IGMP packets send multicast data that they receive for requested groups out the network segment of the known receivers.

By default, when PIM is enabled on an interface, IGMP version 3 is enabled. IGMP can be enabled on an interface explicitly.

IGMP Versions

OcNOS supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception. By default, OcNOS enables IGMPv3 when PIM is enabled on an interface.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following feature:
  - Host messages that can specify both the group and the source.
  - The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

IGMP Operation

IGMP works on the premise of three major packets exchange between IGMP enabled routers and hosts, interested in joining a particular group.

IGMP Query Operation

Once IGMP is enabled or pim is enabled (which enables igmpv3), on any interface it starts sending Query message, which is called general query to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data.

OcNOS elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

In the figure below Router-1 eth2 sends query every query-interval. Since Router1-eth2 IP address is less than Router-2 eth2, Router-1 eth2 becomes querier on the LAN.

IGMP Membership Report Operation

When a host receives a query from the local router it sends a Host Membership Report for all the multicast groups for which it wants to receive multicast traffic. This is called solicited membership report.

When a host joins a new group, the host immediately sends a Membership Report to inform a local router that it wants to receive multicast traffic for the group it has just joined without waiting to receive a Query. This is called unsolicited membership report.

In the figure below Host-1 and Host-2 sends membership reports to Router-1 eth2 for all the multicast groups for which they want to receive multicast traffic. Upon reception of membership report Router-1 maintains an IGMP group table containing multicast group-address, interface name on which it receives the report.

IGMP Leave Operation

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the router sends an IGMP query (Called as Group-specific-query) message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

In the figure below Host-1 and Host-2 sends leave message to Router-1 eth2 for all the multicast groups for which they don’t want to receive multicast traffic. In response to leave message Router-1 eth2 sends an group-specific-query message before removing the multicast group address from the IGMP table.

Topology

The procedures in this section use the topology in Figure 1-69.

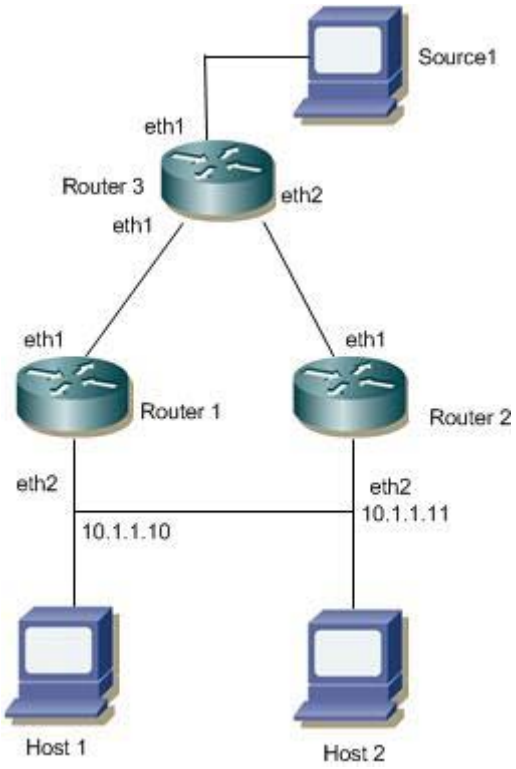


Figure 1-69: IGMP Topology

IGMP Configuration

The following example shows IGMP configuration on Router1.

Configuring IGMP Version

The configuration that follows shows how IGMP version can be configured.

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.1.1.10/24`	Assign IP address to an interface
`(config-if)#ip igmp version 2`	Enable IGMP version as v2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
#show  running-config
!
no service password-encryption
```

```
!
hostname rtr1
!
ip multicast-routing
!
!
interface eth2
ip address 10.1.1.10/24
no shutdown
ip igmp version 2
```

Configuring IGMP Parameters

The configuration that follows shows how IGMP parameters can be configured.

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip igmp access-group 1`	Configures a access-list policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
`(config-if)#ip igmp immediate-leave group-list 1`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
`(config-if#ip igmp  join-group 224.1.1.1`	Statically binds a multicast group to the outgoing interface
`(config-if)# ip igmp  last-member-query-count 7`	Sets the query count used when the software starts up.
`(config-if)# ip igmp  last-member-query-interval 25500`	Sets the query interval used when the software starts up.
`(config-if)#ip igmp limit 100`	Configure Max Allowed State on this interface
`(config-if)#ip igmp querier-timeout 300`	Sets the querier timeout that the router uses when deciding to take over as the querier.
`(config-if)#ip igmp  query-interval 200`	Sets the frequency at which the router sends IGMP host query messages.
`(config-if)#ip igmp  query-max-response-time 150`	Sets the response time advertised in IGMP queries.
`(config-if)#ip igmp  ra-option`	Enable ra-option.
`(config-if)#ip igmp  robustness-variable 4`	Sets the robustness variable.
`(config-if)#ip igmp startup-query-count 4`	Sets the query count used when the router starts up.
`(config-if)# ip igmp startup-query-interval 50`	Sets the query interval used when the router starts up.
`(config-if)# ip igmp static-group 225.1.1.1`	Statically binds a multicast group to the outgoing interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
ip multicast-routing
!
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2
 !!

Rtr1#show  ip igmp   interface  eth2
Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Configured for version 2
Internet address is 10.1.1.10
IGMP interface limit is 100
IGMP interface has 2 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 0, v2-leaves: 0
v3-reports: 0
IGMP query interval is 200 seconds
IGMP Startup query interval is 50 seconds
IGMP Startup query count is 4
IGMP querier timeout is 300 seconds
IGMP max query response time is 150 seconds
Group Membership interval is 950 seconds
IGMP Last member query count is 7
Last member query response interval is 25500 milliseconds
```

Here is the sample configuration on Router-1 with all the IGMP related commands configured.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
```

```
ip domain-lookup
!
ip multicast-routing
!
ip pim register-rp-reachability
ip pim crp-cisco-prefix
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.57/32 secondary
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.179/24
 no shutdown
!
interface eth1
 ip address 192.168.1.27/24
 no shutdown
 ip igmp version 2
 !
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2

!
line con 0
 login
line vty 0 16
 exec-timeout 0 0
 login
line vty 17 39
 login
!
End
```

IGMP Group Table after IGMPV2 Membership Report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-23: IGMP group table after IGMPV2 membership report

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
Rtr1#show  ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime     Expires     State     Last Reporter
224.0.1.3            eth2       00:10:06   00:03:43    Active    10.1.1.52
224.1.1.1            eth2       01:54:53   static      Active    0.0.0.0
225.1.1.1            eth2       00:17:22   static      Active    0.0.0.0
```

```
Rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
State: Active
Last reporter:  10.1.1.52
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          225.1.1.1
```

```
Flags:          SG
Uptime:         00:17:28
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty
```

IGMP Group Table after IGMPV3 Membership report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface. Here IGMPV3 should be configured on the interface (by default IGMPv3 will be enabled if pim is configured on the interface).

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-24: IGMP group table after IGMPV3 membership

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
rtr6#show  ip igmp  groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
224.0.1.3        eth2                 00:08:50 00:02:10 192.168.10.52
rtr6#show  ip igmp  groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:08:50
Group mode:     Exclude (Expires: 00:04:57)
Last reporter:  192.168.10.52
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Exclude Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  1.2.3.4         00:08:50  stopped   No   R

For IGMPV3 report source list specifies which source to be included or exclude
based on the membership report sent by the hosts.

In the above show command, Source address 1.2.3.4 is excluded to send
Multicast data  for group 224.0.1.3
```

CHAPTER 2 IGMP Proxy Configuration

In some simple tree topologies, it is not necessary to configure complex multicast routing protocols, such as PIM, on the boundary devices. It is sufficient to learn and proxy the group membership information and simply forward multicast packets based upon that information. Using IGMP forwarding (RFC 4605) to replicate multicast traffic on devices such as the edge boxes can greatly simplify the design and implementation of those devices. By not supporting more complicated multicast routing protocol such as Protocol Independent Multicast (PIM), it reduces not only the cost of the devices but also the operational overhead. Another advantage is that it makes the proxy devices independent of the multicast routing protocol used by the core network routers.

IGMP proxy can be used in such topologies instead of PIM. With IGMP proxy configured, the device serves as a proxy for the downstream hosts to send IGMP messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device configured with IGMP proxying is a host but no longer a PIM neighbor to the upstream device.

A device with IGMP proxy configured maintains a group membership database, which stores the group memberships on all the downstream interfaces. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to queries according to the information in the database or sends join/leave messages when the database changes. On the other hand, the proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

Terminology

Following is a brief description of terms and concepts used to describe the IGMP Proxy:

Upstream interface

Also referred to as the proxy interface. A proxy interface is an interface on which IGMP proxy service is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host running IGMP; therefore, it is also called host interface.

Downstream interface

An interface that is running IGMP and in the direction contrary to the root of the multicast forwarding tree. A downstream interface acts as a router running IGMP; therefore, it is also called router interface.

Member State

State of the associated group address and interface.

- Idle - Interface has not yet responded to a group membership query or general query for this group.
- Delay - Interface has responded to the latest group membership query or general query for this group.

IGMP-Proxy Configuration Steps

This section provides the configuration steps for configuring IGMP Proxy and example for a relevant scenario.

- Enable IP multicast on each router (see Enabling IP Multicast Routing)
- Enable IGMP Proxy service on the upstream interface.
- Enable IGMP mroute configuration on the downstream interface.
- Enable IGMP proxy unsolicited report interval on the proxy interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time. This is an optional parameter in which the default value of 1 sec is considered for forwarding proxy groups to upstream router.

Note: Configure IP addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

In this network topology, Router 1 acts as a proxying router to the upstream router Router 2 in which PIM domain is present. Also the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

Note: Any PIM mode (PIM-SM,PIM-DM,PIM-SMDM) should be enabled on all the interfaces in the PIM domain.

Here in this example default value for unsolicited report interval is considered.

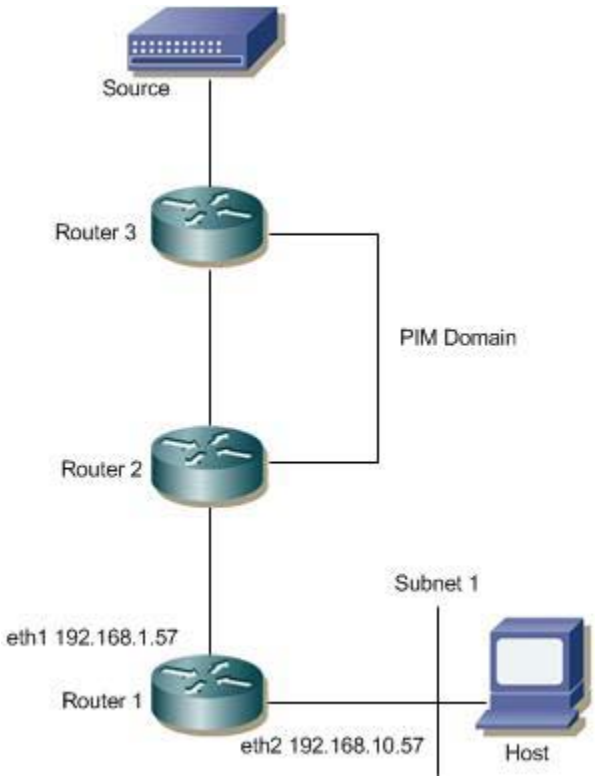


Figure 2-70: IGMP Proxy Topology

In this example, Routers 2 and 3 are running PIM and Router1 is the IGMP Proxying router.

- Host ends an IGMP membership report to Subnet 1.
- Downstream interface on Router1 received IGMP reports from host and updates the proxy interface.

- IGMP Proxying router (Router1) maintains the group membership information and forwards the received report to the upstream router (Router2).
- Source then sends a data packet for group.
- When the data packet reaches Router1, it forwards via the interface, eth2, because it has an IGMP join requested for Multicast traffic.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)# ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling Proxy upstream interface

Enable IGMP proxy service on the interface in which the interface is in the direction toward the root of the multicast forwarding tree. In this example eth1 is the upstream interface which acts as an IGMP host.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 192.168.1.57/24`	Assign IP address to an interface
`(config-if)#ip igmp proxy-service`	Enable IGMP proxy service on the upstream interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Enabling Proxy downstream interface

Enable IGMP mroute proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Enter Interface mode
`(config-if)#ip address 192.168.10.57/24`	Assign IP address to an interface
`(config-if)#ip igmp mroute-proxy eth1`	Enable IGMP mroute proxy on the downstream interface and specify the upstream proxy interface name.
`(config-if)#exit`	Exit Interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface lo
!!
ip multicast-routing
!
interface eth0
!
interface eth1
 ip address 192.168.1.57/24
 no shutdown
 ip igmp proxy-service
!
interface eth2
 ip address 192.168.10.57/24
 no shutdown
 ip igmp mroute-proxy eth1
!
```

IGMP proxy interface

The following output displays the IGMP Proxy interface information.

```
Router1#show ip igmp interface

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 1000 milliseconds


Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Version 3 (default)
 IGMP mroute-proxy interface is eth1
 Internet address is 192.168.10.57
 IGMP interface has 1 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 1, v2-leaves: 0
v3-reports: 0
IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
```

IGMP proxy

The following output displays the IGMP proxy information.

```
Router1#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
```



```
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1
```

IGMP proxy groups

The following output displays the IGMP proxy group membership information.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

Enabling Unsolicited report interval

Enable IGMP proxy unsolicited report interval on the upstream interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)#ip igmp proxy unsolicited-report-interval 20000`	Enable IGMP proxy unsolicited report interval value on the upstream interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface eth0
!
```

```
interface eth1
ip address 192.168.1.57/24
ip igmp proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface eth2
ip address 192.168.10.57/24
ip igmp mroute-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

The following output displays the IGMP proxy unsolicited report interval information.

```
Router1#show ip igmp interface eth1

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 20000 milliseconds
```

IGMP proxy group with unsolicited report interval

The following output displays the IGMP proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Idle
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```


CHAPTER 3 PIM Sparse Mode Configuration

The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps geographically dispersed network nodes to conserve bandwidth and reduce traffic by simultaneously delivering a single stream of information to multiple locations. PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-SM protocol:

Rendezvous Point

A Rendezvous Point (RP) router is configured as the root of a non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB decides where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link, once in each direction.

Tree Information Base

The Tree Information Base (TIB) is a collection of states at a PIM router storing the state of all multicast distribution trees at that router. The TIB is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Upstream indicates that traffic is going towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Downstream indicates that traffic is going away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In Source-Based Trees, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric used is `hop counts`, the branches of the multicast Source-Based Trees are minimum hop. If the metric used is `delay`, the branches are minimum delay. A corresponding multicast tree directly connects the source to all receivers for every multicast source. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces -- the source address and the multicast group.

Shared Trees

Shared trees, or RP trees (RPT), rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists. The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Note: Not all hosts are receivers.

Bootstrap Router

When a new multicast sender starts sending data packets, or a new receiver starts sending Join messages towards the RP for that multicast group, the sender needs to know the next-hop router towards the RP. The bootstrap router (BSR) provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

Data Flow from Source to Receivers in PIM-SM Network Domain

1. Sending out Hello Messages

   PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address, 224.0.0.13 (`ALL-PIM-ROUTERS` group). Routers do not send any acknowledgement that a Hello message was received. A `holdtime` value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

2. Electing a Designated Router

   In a multi-access network with multiple routers connected, one of the routers is selected to act as a designated router (DR) for a given period. The DR is responsible for sending Join/Prune messages to the RP for local members.

3. Determining the Rendezvous Point

   PIM-SM uses a BSR to originate bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements.

The router with the highest priority (if priorities are same, the higher IP address applies) is selected to be the RP. Routers receive and store bootstrap messages originated by the BSR. When a DR gets a membership indication from IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the designated router (DR) maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP. In a small domain, the RP can also be configured statically.

4. Joining the Shared Tree

   To join a multicast group, a host sends an IGMP message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIM neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

5. Registering with the RP

   A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP de-encapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT. Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IP multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice. When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

6. Sending Register-Stop Messages

   When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IP packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IP multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

7. Pruning the Interface

   Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

8. Forwarding Multicast Packets

   PIM-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork, and have a Time to Live (TTL) of one (1). The router performs an RPF check, and forwards the packet. If a downstream router has sent a join to this router or is a member of this group, then traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers.

PIM-SM Configuration

PIM-SM is a soft-state protocol. The required steps to configure PIM-SM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SM on the desired interfaces (see Enable PIM-SM on an Interface)
- Configure the RP statically (see Configuring Rendezvous Point Statically or dynamically (see Configure Rendezvous Point Dynamically Using Bootstrap Router Method) depending on which method you use)

All multicast group states are dynamically maintained as the result of IGMP `Report/Leave` and PIM `Join/Prune` messages.

This section provides the steps to configure the PIM-SM feature. Configuration steps and examples are used for two relevant scenarios.

Topology

The following figure displays the network topology used in these examples.

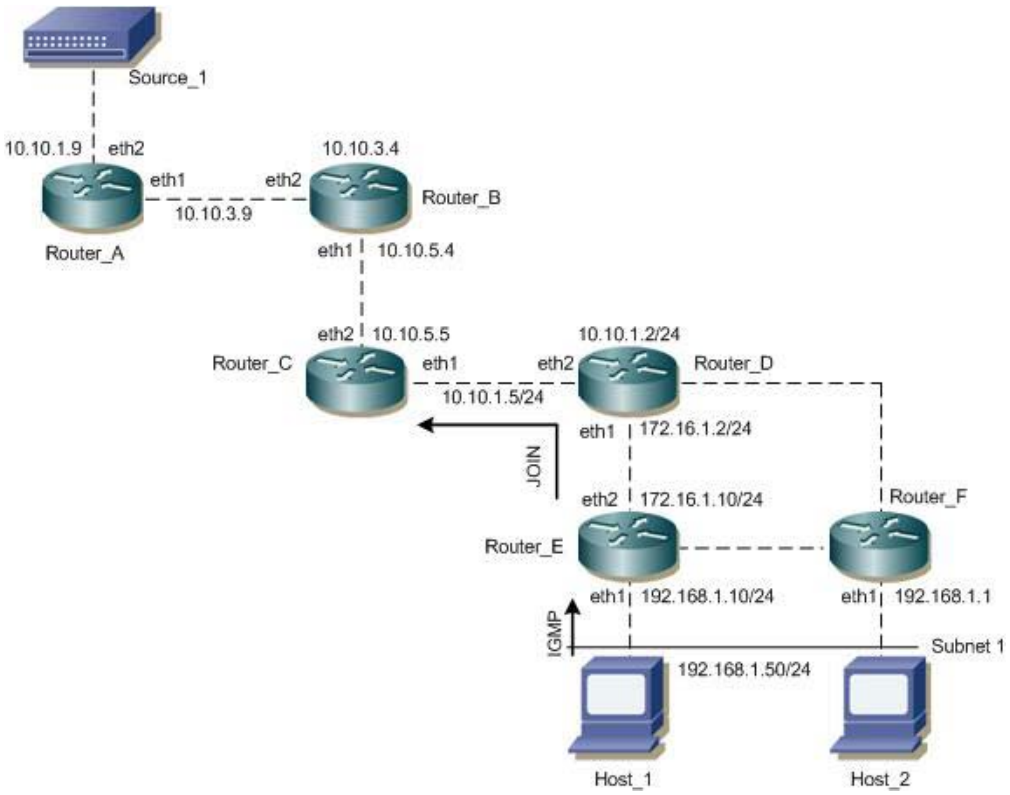


Figure 3-71: PIM-SM Topology

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

Enable IP Multicast Routing

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enable PIM-SM on an Interface

Enable PIM-SM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SM on the router.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and Enter interface mode.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured and Enter interface mode.
`(config-if)#ip address 10.10.13.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit interface mode.

Configuring Rendezvous Point Statically

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address with in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 3-71, `Router_C` is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, `Router_E` and `Router_F`; both have default DR priority on `eth1`.

Since Router_E has a higher IP address on interface eth1, it becomes the Designated Router, and is responsible for sending Join messages to the RP (Router_C).

Configure Static RP

#configure terminal	Enter configure mode.
(config)#ip pim rp-address 10.10.1.5	Statically configure an RP address for multicast groups.
(config)#exit	Exit Configure mode.

Here is the sample configuration for Router_D:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing

ip pim rp-address 10.10.1.5
!
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

RP Details

At Router_D, the show ip pim rp mapping command shows that 10.10.1.5 is the RP for all multicast groups 224.0.0.0/4, and is statically configured. All other routers will have a similar output:

```
R-D#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0


Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:19:31
R-D#
```

Override RP cnt: 0At Router_D, use the show ip pim rp-hash command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.1.5
```


Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1.`

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

```
R-E#show ip pim mroute
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     i.............................
 Joined    .............................
 Asserted  .............................
FCR:

R-E#
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and `eth1` is on the outgoing interface list of the (*, G) entry. This means that there is a group member through `eth1`, and the RP is reachable through `eth2`.

The 0 position on this 32-bit index is for `eth1` (as illustrated in the interface display above). The `j` on the 0 index indicates that the `Join` has come from `eth1`.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
R-C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.3)
```

```
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
FCR:

R-C#
```

Configure Rendezvous Point Dynamically Using Bootstrap Router Method

A static RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and/or complex one. In such a network, if the RP fails or you have to change the assignment of the RP, you are required to reconfigure the static configurations on all PIM routers. Also, if you have several multicast groups mapped to several RPs, there are many repetitive configurations you are required to perform, which can be time consuming and laborious. Thus when it comes configuring RP in large and/or complex networking environments, configuring it dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the RP dynamically.

The BSR mechanism in a PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-to-RP mappings required in order to function. The BSR's function is to broadcast the RP set to all routers in the domain.

Some of the PIM routers within a PIM domain are configured as Candidate-RPs (C-RPs). A subset of the C-RPs is eventually used as the actual RPs for the domain. An RP configured with a lower value in the priority field has a higher priority.

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies to the elected BSR, which chooses a subset of the C-RPs, and distributes corresponding group-to-RP mappings to all the routers in the domain using Bootstrap messages.

This section provides 2 examples to illustrate the BSR configuration for configuring RP dynamically.

Example 1

For this example, refer to Figure 1 for the topology.

To dynamically configure the RP, `Router_C` on `eth1` and `Router_D` on `eth1` are configured as a Candidate RP using the `ip pim rp-candidate` command. `Router_D` on `eth1` is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, `Router_D` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP to ensure that all routers in the PIM-domain have the same RP for the same group.

To change the default priority of any candidate RP, use the `ip pim rp-candidate IFNAME PRIORITY` command. At `Router_D`, the `show ip pim rp mapping` command shows that `Router_C` is chosen as the RP for a specified group.

Configure RP Dynamically for Router C

`#configure terminal`	Enter configure mode.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

Configure RP Dynamically for Router D

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1`	Give this router the candidate BSR status using the name of the interface.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

The following output displays the complete configuration at `Router_C` and `Router_D`:

```
Router_D#show running-config
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
ip multicast-routing
ip pim bsr-candidate eth1
ip pim rp-candidate eth1 priority 2
!

Router_C#show running-config
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-candidate eth1
```

Validation

This section provides the steps to verify the RP configuration.

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about RP candidates. There are two RP candidates for the group range, 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group, 224.0.0.0/4.

```
R-D#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:02:24, expires: 00:02:11
  RP: 10.10.1.5
    Info source: 10.10.1.5, via bootstrap, priority 2
         Uptime: 00:02:26, expires: 00:02:06
Override RP cnt: 0


Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:55:25
R-D#
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states, as a result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the *Configuring Rendezvous Point Statically* section.

Example 2

To dynamically configure the RP, `Router_2` on `eth1` is configured as a Candidate RP using the `ip pim rp-candidate` command. Since no other router is configured as C-RP, `Router_2` becomes the RP. `Router_1` on `eth1` and `Router_2` on `eth1` are configured as the Candidate BSRs. Since `Router_1` has a higher priority value than `Router_2`, `Router_1` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

For this example, refer to Figure 3-72 for the topology.

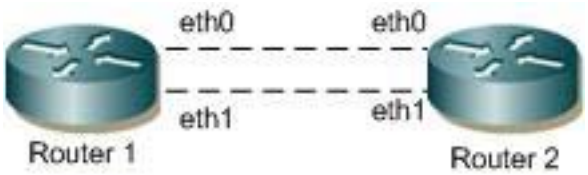


Figure 3-72: Boostrap Router Topology

Configuration

Router 1

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1`	Configure `eth1` of Router 1 as C-BSR. The default priority is 64, so it is not necessary to designate a priority.
`(config)#exit`	Exit Configure mode.

Router 2

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1 10 25`	Configure `eth1` of Router 2 as C-BSR with a hash mask length of 10, and a priority of 25.
`(config)#ip pim rp-candidate eth1 priority 0`	Configure interface `eth1` as C-RP with a priority of 0.
`(config)#exit`	Exit Configure mode.

Router 2 Unicast BSM

When the `ip pim unicast-bsm` command is configured on an interface that is a DR for a network, then that interface unicasts the stored copy of BSM to the new or rebooting router.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip pim dr-priority 10`	Configure `eth1` as DR
`(config-if)#ip pim unicast-bsm`	Enable sending and receiving of Unicast BSM for backward compatibility.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the C-BSR state on Router 1.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 20.0.1.21
  Uptime:      00:01:39, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:53
```

```
  Role: Candidate BSR
  State: Elected BSR
```

2. Verify the C-BSR state on Router 2.

   The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 20.0.1.21
  Uptime:      00:02:39, BSR Priority: 64, Hash mask length: 10
  Expires:     00:00:03
  Role: Candidate BSR
  State: Pending BSR

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
Candidate RP: 20.0.1.11(eth2)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:02
    Backoff cnt 1

#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.21, via bootstrap, priority 0
         Uptime: 00:02:17, expires: 00:02:26
Override RP cnt: 0
```

3. Verify RP-set information on E-BSR.

```
R1#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.11, via bootstrap, priority 0
         Uptime: 00:00:22, expires: 00:02:12
Override RP cnt: 0
```

4. Verify RP-set information on C-BSR.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP  1.1.1.152 members :
```

```
  4.4.4.5   7.7.7.1   23.23.23.1

Group(s): 224.0.0.0/4, Static
    RP: 1.1.1.152
         Uptime: 00:00:37
ARP1#
```

Anycast-RP Configuration

The Anycast-RP feature provides load balancing among active RPs and redundancy in a PIM-SM network domain. In a PM-SM configuration, only a single active RP for each multicast group within a domain is permitted. However, in an Anycast-RP configuration, this restriction is removed with the support of multiple active RPs for each group in a domain.

OcNOS supports Anycast-RP using the PIM implementation. In PIM Anycast-RP, Multicast Source Discovery Protocol (MSDP) is not employed to share information about active sources. Instead the Register mechanism in PIM is extended to provide this same function.

The following describes Anycast-RP in PIM-SM:

- A Unicast IP address is used as the RP address. The address is statically configured, and associated with all PIM routers throughout the domain.
- A set of routers in the domain is chosen to act as RPs for this RP address. These routers are called the Anycast-RP set.
- Each router in the Anycast-RP set is configured with a loopback address. The loopback address is configured on all RPs for the loopback interface, then configured as the RP address (static RP), and injected into OSPF using redistribute connected. The PIM-SM implementation uses only the first non-loopback address configured on the loopback interface. Therefore, it is important to be sure that the Anycast-RP address is configured with the first non-loopback address.
- Each router in the Anycast-RP set also needs a separate IP address, which is used for communication between the RPs.
- The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.

Topology

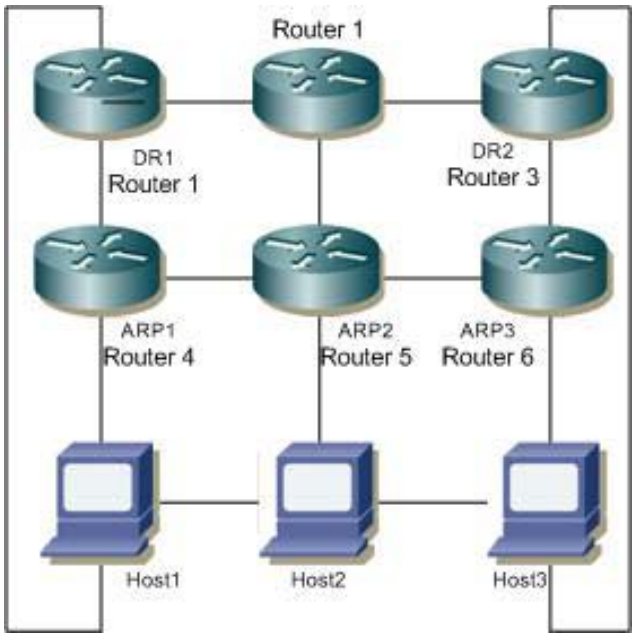


Figure 3-73: Anycast RP Topology

Host1 and Host3 act as hosts and sources for sending join and multicast data packets; Host2 acts as a host.

ARP1, ARP2 and ARP3

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter the loopback interface.
`(config)#ip address 1.1.1.152/32 secondary`	Configure the IP address for loopback
`(config)#exit`	Exit the Configure mode.
`(config)#ip pim rp-address 1.1.1.152`	Configure the static RP with the address of the loopback.
`(config)#ip pim anycast-rp 1.1.1.152 4.4.4.5`	Configure the member RP address. In this example, `4.4.4.5` is the member RP in ARP2. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 7.7.7.1`	Configure the member RP address. In this example, `7.7.7.1` is the member RP in ARP3. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 23.23.23.1`	Configure the member RP address. In this example, `23.23.23.1` is the member RP in ARP1. It is the address used for communication between all RPs.
`(config)#exit`	Exit the Configure mode.

Disable Anycast-RP

`#configure terminal`	Enter configure mode.
`(config)#no ip pim anycast-rp 1.1.1.152`	Disable Anycast-RP.
`(config)#no ip pim rp-address 1.1.1.152`	Disable static RP.
`(config)#exit`	Exit Configure mode.

Validation

1. Verify RP-mapping in ARP1.

```
#show ip pim rp mapping
      PIM Group-to-RP Mappings
      Override RP cnt: 0
      Anycast-RP 1.1.1.152 members:23.23.23.1
      Group(s): 224.0.0.0/4, Static
      RP: 1.1.1.152
        Uptime: 00:00:13s
```

2. Verify RP-mapping in ARP1 after disabling anycast-RP and RP-address.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP  1.1.1.152 members :
  4.4.4.5   7.7.7.1   23.23.23.1

Group(s): 224.0.0.0/4, Static
    RP: 1.1.1.152
         Uptime: 00:00:37
ARP1#
```

CHAPTER 4 PIM Dense Mode Configuration

Protocol Independent Multicast - Dense Mode (PIM-DM) is a data-driven multicast routing protocol that builds source-based multicast distribution trees that operate on the flood-and-prune principle. PIM-DM requires unicast-reachability information, but it does not depend on a specific unicast routing protocol.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-DM protocol:

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only when `IF1` is the interface the router would use in order to reach `SourceA`. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Forwarding Multicast Packets

PIM-DM routers forward multicast traffic to all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers, if the downstream router is a member of this group.

Upstream

Upstream traffic is traffic that is going towards the source.

Downstream

Downstream traffic is anything other than the upstream interface for that group.

Nexthop

PIM-DM does periodic lookups for prefixes to check router reachability. The nexthop lookup mechanism avoids periodic lookup. During start-up, PIM-DM notifies NSM (Network Services Manager) about the prefixes that pertain to them. NSM notifies the protocols if a better nexthop is available, or if a nexthop becomes unavailable. In this way, PIM-DM does not expend resources to do periodic lookups, because NSM is proactive in their maintenance.

Configuration

Configuring PIM-DM requires the following steps:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)

- Enable PIM-DM on the desired interfaces (see Enabling PIM-DM)

This section provides the configuration steps for configuring PIM-DM and examples for a relevant scenario.

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

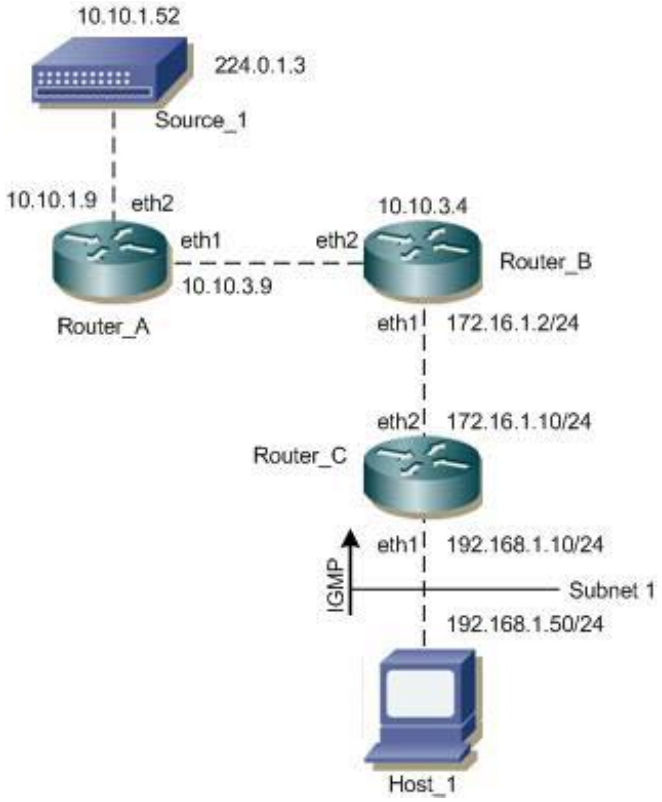


Figure 4-74: PIM-DM Configuration Topology

In this example, all routers are running PIM-DM.

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, `eth1`, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches `Router_C`, it forwards via the interface, `eth1`, because there is a local member on this interface for this group. `Router_C` has a downstream receiver, so it does not send a prune message to its upstream neighbor router, `Router_B`.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

#configure terminal	Enter Configure mode.
(config)#ip multicast-routing	Enable IP multicast routing.
(config)#exit	Exit Configure mode.

Enabling PIM-DM

Enable PIM-DM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM.

#configure terminal	Enter Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.15.12/24	Configure the IP address for eth1.
(config-if)#ip pim dense-mode	Enable PIM dense mode on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 10.10.14.12/24	Configure the IP address for eth1.
(config-if)#ip pim dense-mode	Enable PIM dense mode on the interface.
(config-if)#exit	Exit interface mode.

The following is a sample configuration for Router_C:

```
hostname Router_C
!
interface eth0
!
interface eth1
 ip pim dense-mode
!
interface eth2
 ip pim dense-mode
!
interface lo
!
!
ip multicast-routing
!
```

Validation

The show ip pim interface command displays the interface details for Router_C.

```
Router_C#show ip pim interface
Address          Interface VIFindex Ver/   Nbr     DR
                                    Mode   Count   prior
192.168.1.10      eth1      0       v2/D   0        1
172.16.1.10       eth2      2       v2/D   1        1
```

The `show ip mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
 Incoming interface: eth2
 Outgoing interface list:
    eth1 (1)
```

The `show ip pim mroute` displays the IP PIM-DM multicast routing table.

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table
(10.10.1.52, 224.0.1.3)
 RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
 Upstream IF: eth2
    Upstream State: Forwarding
    Assert State: NoInfo
 Downstream IF List:
    eth1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

CHAPTER 5 IGMP Snooping Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP) Snooping.

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Without IGMP, Layer-2 switches handle IP multicast traffic in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP Snooping is enabled on the switches.

Topology

This example describes the configuration on switch S1. The eth1 interface is configured as a multicast router port.

Because IGMP Snooping is used in bridged LAN environments, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

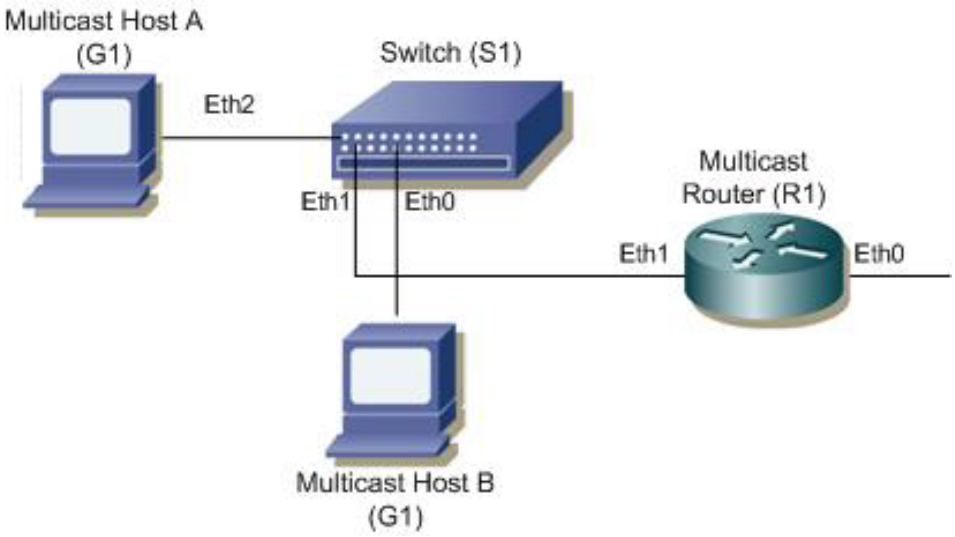


Figure 5-75: IGMP Snooping Topology

As a result of this configuration:

- The switch itself replies with membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch, when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when A leaves the group, because the group still has another member. When Host B leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

Configuration

To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table

2. Specify the interface to be configured
3. Associate the interface with bridge group
4. IGMP snooping will be enabled by default
5. Configure ports that are connected to routers as multicast router ports
6. By default, IGMP report suppression is enabled on the switch

S1

`#configure terminal`	Enter the `Configure` mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Add bridge `1` to the spanning-tree table.
`(config)#interface eth0`	Specify the interface `eth0` to be configured, and enter the `Interface` mode.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `eth1` with bridge-group `1.`
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth1`	Specify interface `eth1` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth2`	Specify interface `eth2` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth2` with bridge-group `1.`
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface vlan1.1`	Specify interface `vlan1.1` to be configured.
`(config-if)# igmp snooping mrouter interface eth1`	Configure this port as a multicast router port
`(config-if)#exit`	Exit the `Interface` mode

Validation

```
#show running-config interface eth0
!
interface eth0
```

```
switchport
bridge-group 1
switchport mode access
!
#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode access
!

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode access
!

#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan Group/Source Address Interface Flags Uptime Expires Last Reporter Version
1 224.1.1.1 eth0 R 00:00:03 00:04:17 0.0.0.0 V3
1 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0 V3

#show igmp snooping interface vlan1.1
IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 1
Number of Groups: 1
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 2
Active Ports:
eth0
eth1
eth2
```

CHAPTER 6 MSDP Configuration

Multicast Source Discovery Protocol (MSDP) is used to exchange multicast source information between BGP-enabled PIM-SM domains. Using MSDP, routers in a PIM-SM domain can rely on their own RP to reach a source in a different PIM-SM domain.

Overview

MSDP routers in a PIM-SM domain have a MSDP peering relationship with MSDP peers in another domain using a TCP connection. MSDP peering is the first step towards exchanging inter-domain multicast source information using MSDP SA (Source-Active) messages.

When an RP in a PIM-SM domain first learns of a new sender (via PIM register messages), it constructs an SA message and sends it to its MSDP peers.

All RPs which intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer.

An SA message contains these fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Each SA message received from a MSDP peer goes through an RPF check. The peer-RPF check compares the RP address carried in the SA message with the MSDP peer from which the message was received:

- If the MSDP peer receives an SA from a non-RPF peer towards the originating RP, it drops the message.
- Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an RP receives a new SA message from a peer in another domain, it checks if there are any receivers interested in the traffic. An RP checks for a (*, G) entry with a non-empty outgoing list. If the outgoing list is non-empty, the RP sends a (S,G) join towards the source.

Caching SA state

If a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to learn about the source. MSDP SA caching is done at MSDP peers to reduce join latency for new receivers. The SA cache is populated as soon an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

MSDP Mesh groups are used inside a PIM-SM domain to ease RPF checking and SA forwarding within the domain. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. This reduces SA message flooding and simplifies peer-RPF flooding.

MSDP Default Peer

An MSDP default peer is used when MSDP peers are not BGP peers. SA messages coming from a default peer do not go through an RPF check and are always accepted.

Configure PIM-SM

For the MSDP topology in Figure 6-76, you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see Chapter 3, *PIM Sparse Mode Configuration*.

Configure MSDP

In the topology in Figure 6-76, an MSDP session is established between RTR-1 and RTR-2 in both domains. The following sample configuration on RTR-1 shows how to enable MSDP peering between RTR-1 and RTR-2.

Topology

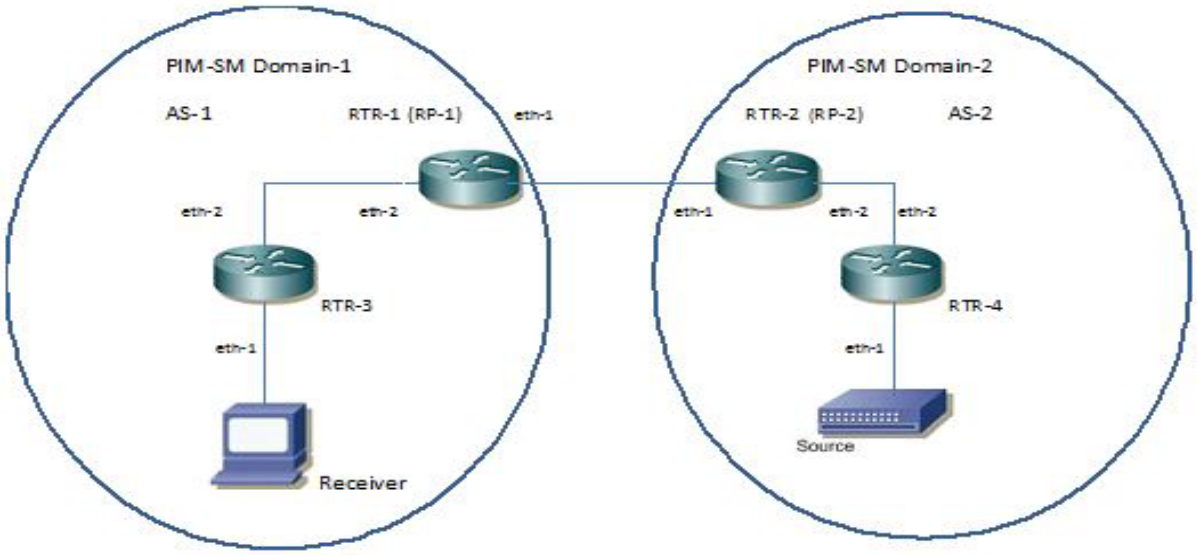


Figure 6-76: MSDP topology

IP addresses:

- RTR-1 eth1: 11.1.1.11
- RTR-1 eth2: 10.1.1.11
- RTR-2 eth1: 11.1.1.12
- RTR-2 eth2: 12.1.1.12
- RTR-4 eth1: 12.1.1.14
- RTR-4 eth2: 20.1.1.14

RTR-3 eth1: 13.1.1.13

RTR-3 eth2: 10.1.1.13

Source: 20.1.1.10

Multicast group: 224.1.1.1

RTR-1

`#configure terminal`	Enter configure mode.

`(config)#ip msdp peer 11.1.1.12`
--or--
`(config)#ip msdp peer 11.1.1.12 connect source eth1`
	Configure a MSDP peer.
	
	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.

`(config)#ip msdp password myPass peer 11.1.1.12`	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
`(config)#ip msdp default-peer 11.1.1.12`	Configure MSDP default peer.
`(config)#ip msdp mesh-group mesh1 11.1.1.12`	Configure MSDP mesh group.
`(config)#ip msdp originator-id eth2`	Configure MSDP originator identifier.
`(config)#exit`	Exit configure mode.

Validation

RTR-1

```
#show running-config

ip msdp peer 11.1.1.12
ip msdp default-peer 11.1.1.12
ip msdp mesh-group mesh1 11.1.1.12
ip msdp password myPass peer 11.1.1.12
ip msdp originator-id eth2
ip multicast-routing
!
ip pim register-rp-reachability
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
ip pim vrf management register-rp-reachability
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.175/24
 no shutdown
!
```

```
interface eth1
 ip address 11.1.1.11/24
no shutdown
 ip pim sparse-mode
ip pim bsr-border
!
interface eth2
 ip address 10.1.1.11/24
 no shutdown
ip pim sparse-mode
!
interface eth3
 no shutdown
!
interface pimreg
 no multicast
 no shutdown
!
router ospf 100
 network 10.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 1
neighbor 11.1.1.12 remote-as 2
!
line con 0
 login
line vty 0 39
 login
!
```

This command shows the MSDP peer information at RTR-1:

```
#show ip msdp peer
MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

In the MSDP topology in Figure 6-76, when a source sends multicast traffic for group 224.1.1.1, RTR-4 (the DR) sends a register packet towards RTR-2 which is the RP in the domain. RTR-2 receives the register packet and sends an MSDP SA message to its MSDP peer (RTR-1). RTR-1 receives the SA message and creates an entry in the SA cache containing the source, group, and RP information.

This command at RTR-1 shows the SA information with source address, group address, and RP address:

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02 Exptime
00:03:28P
```

RTR-3 receives an IGMP join for group 224.1.1.1 and joins the shared tree path toward the RP (RTR-1).

When RTR-1 receives an SA message from RTR-2, because it has a receiver, it sends an (S,G) join towards the source. Now traffic from the source is received at RTR-1 via the shortest path tree formed between RTR-1 and the source. RTR-1 distributes traffic downstream towards the receiver.

This command shows the PIM state at RTR-1 upon receiving an SA message and joining towards the source:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 224.1.1.1)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 11.1.1.12
RPF idx: eth1
SPT bit: 0
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o.............................

(20.1.1.10, 224.0.1.3, rpt)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ................................
 Pruned    ................................
 Outgoing  ..o.............................
```

RTR-2

This command shows the MSDP peer information at RTR-2.

```
#show  ip msdp  peer
MSDP Peer 11.1.1.11
Connection status
 State: Up (Established)
 Keepalive sent: 2
```

```
Keepalive received: 2
```

CHAPTER 7 Bidirectional-PIM Configuration

Bidirectional PIM (BIDIR-PIM) is a variant of PIM Sparse-Mode (PIM-SM) that builds bidirectional shared trees connecting multicast sources and receivers as specified in RFC5015.

BIDIR-PIM dispenses with both encapsulation and source state by allowing packets to be natively forwarded from a source to the Rendezvous Point (RP) using shared tree state.

BIDIR-PIM uses the same tree for traffic from source towards RP and from RP to receivers.

Note: BIDIR-PIM with BSR is not supported in OcNOS 4.0.

Designated Forwarders (DF) Election

Bidirectional Shared-Trees violates current (*, G) RPF rules, as it accepts traffic from one Reverse Path Forwarding (RPF) interface only. To avoid forwarding multicast packet looping, bidir-PIM introduces a new mechanism called the designated forwarder (DF) election.

The designated forwarder (DF) election takes place for all PIM routers on every network segment and point-to-point link. The procedure selects one router as the DF for every RP of bidirectional groups. The designated forwarder is responsible for forwarding multicast packets received on that network.

PIM-SM Configuration

For the steps to configure PIM-SM refer to PIM Sparse Mode Configuration on page 2551.

Enabling BIDIR-PIM

`#configure terminal`	Enter Configure mode.
`(config)#ip pim bidir-enable`	Enable bidir-pim
`(config)#exit`	Exit Configure mode.

Configuring BIDIR Rendezvous Point Statically

Configuring Static BIDIR RP

`#configure terminal`	Enter configure mode.
`(config)#ip access-list standard ip1` `(config-ip-acl-std)#permit 224.0.0.0/24`	Configure the access list for multicast group.
`(config)#ip pim rp-address 10.10.1.5 ip1 bidir`	Statically configure an rp address for multicast groups.
`(config)#exit`	Exit configure mode.

Here is the sample configuration for Router_D:

```
hostname Router_D
!
       ip access-list standard ip1
        permit 224.0.0.0/24
      !
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
      ip multicast bidirectional enable
!
ip pim bidir-enable
ip pim rp-address 10.10.1.5 ip1 bidir
!
```

Validation

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `22.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5 bidir
         Uptime: 00:01:45
```

At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.5.37
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1.`

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr`	Displays the unicast next-hop to reach RP.
	and mask length.
`RPF idx`	Displays the incoming interface for this (*, G) state.
`RP`	Displays the IP address for the RP router
`B`	Displays the bidirectional pim mode
`The leading dots ....`	
	Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
 Local     ..............................
 Joined    j.............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and the RP is reachable through `eth2`. The ‘B’ flag indicates that it is in bidirectional pim mode.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
 Local     ..............................
 Joined    j.............................
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface (TTL)

(*, 224.0.1.3), uptime 00:00:07, stat expires 00:03:23
Owner PIM, Flags: TFB
  Outgoing interface list:
    eth2 (1)
    eth1 (1)
```

Configuring BIDIR-Neighbor Filter

This section shows how to configure a bidir-neighbor filter to specify which bidirectionally capable (bidir-capable) neighbors will participate in the designated forwarder (DF) election.

`#configure terminal`	Enter configure mode
`(config)# interface eth1`	Enter interface mode
`(config-if)# ip pim bidir-neighbor-filter Acl-name/acl-no`	Configure bidir-neighbor-filter at interface
`(config-if)# no ip pim bidir-neighbor-filter acl-name/acl-no`	Unconfigure bidir-neighbor-filter at interface

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
rtr6#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
192.168.1.149   eth1               00:00:44/00:01:31         v2    1 / B
192.168.1.152   eth1               00:00:01/00:01:44         v2    1 / DR  ------
--?B Flag is removed

rtr6#show running-config interface eth1
!
interface eth1
 ip address 192.168.1.57/24
 no shutdown
 no snmp trap link-status
 ip ospf cost 10
 ip pim bidir-neighbor-filter 1
 ip pim sparse-mode
 lldp-agent
 no dcbx enable
 exit
```

Configuring BIDIR PIM Offer Message Interval Time

This section shows how to configure BIDIR PIM offer message interval time.

`#configure terminal`	Enter configure mode.

`(config)# ip pim bidir-offer-interval <1>`	Specify offer-interval in the range 1-20000
`(config-if)# no ip pim bidir-offer-interval`	Disable offer-interval

Validation

1. Verify the time set for offer message interval

```
(config)#ip pim  bidir-offer-interval 10

#show  running-config
!
no service password-encryption
!
debug nsm packet
debug ip pim events
debug ip pim mfc
debug ip pim packet
debug ip pim state
debug ip pim timer
debug ip pim mib
!
ip vrf management
!
mpls propagate-ttl
!
no ip icmp-broadcast
!
ip multicast-routing
ip multicast bidirectional enable
!
ip pim bidir-enable
ip pim bidir-offer-interval 10
ip pim rp-address 172.31.5.153 bi
```

2. Verify neighbor information in Bidirectional PIM mode with “B” flag associated

```
rtr6#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
192.168.1.149   eth1               00:38:36/00:01:39         v2    1 / B
192.168.1.152   eth1               00:37:53/00:01:22         v2    1 / DR B
rtr6#
```

3. Verify DF status per interface

```
rtr6#show ip pim interface df
Interface RP               DF Winner        Metric
eth1      172.31.5.153     192.168.1.152    20
eth2      172.31.5.153     192.168.10.57    30
rtr6#
rtr6#show ip pim interface eth1 df 172.31.5.153

 Designated Forwarder election for eth1, 192.168.1.57, RP 172.31.5.153
 State                          Non-DF (Lose)
```

```
 Offer count is                  0
 Current DF ip address           192.168.1.152
 Last winner metric preference   110
 Last winner metric              20
rtr6#
```

Configuring BIDIR PIM Offer Interval Limit

This section shows how to configure the Protocol Independent Multicast (PIM) bidirectionally capable number of unanswered offers before it changes as the designated forwarder (DF).

`#configure terminal`	Enter Configure mode.
`(config)# ip pim bidir-offer-limit <offer packet limit>`	Configure bidir-offer-limit
`(config-if)# no ip pim bidir-offer-limit`	Disable offer-limit

Validation

```
rtr6#show  running-config
!
no service password-encryption
!
hostname rtr6
!
!
debug nsm packet
!
ip vrf management
!
mpls propagate-ttl
!
no ip icmp-broadcast
!
access-list 1 deny 192.168.1.152
access-list 1 permit any

!
ip multicast-routing
!
ip pim bidir-enable
ip pim bidir-offer-limit 5
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
```

CHAPTER 8 VRRP Aware PIM Configuration

VRRP Aware PIM is a redundancy mechanism for the Protocol Independent Multicast to interoperate with the Virtual Router Redundancy Protocol. It helps PIM to track VRRP state changes and to preserve multicast traffic upon failover. In order to ensure that the PIM DR is always able to forward PIM Join/Prune message towards RP, the VRRP master router becomes the PIM DR.

Topology

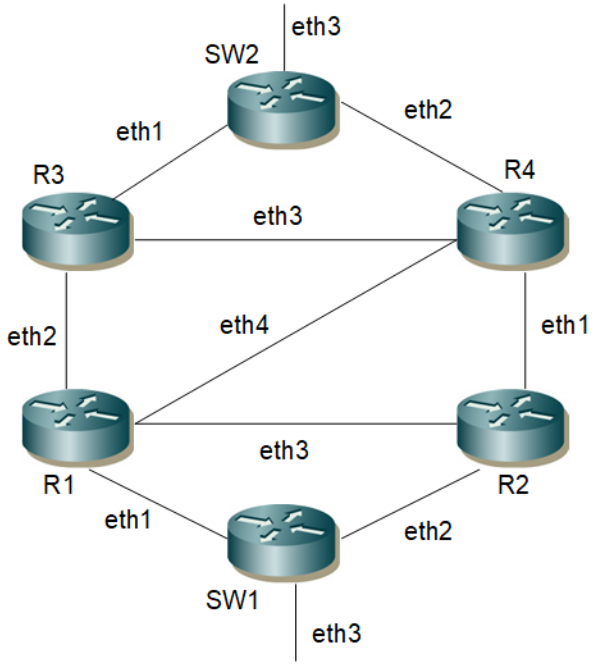


Figure 8-77: VRRP Aware PIM Topology

In the configs below IGMP host is towards SW1 and source is towards SW2.

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`SW1(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`SW1(config)#interface eth1`	Enter interface mode.
`SW1(config-if)#switchport`	Configure eth1 as a layer 2 port.
`SW1(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW1(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW1(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth2`	Enter interface mode.

SW1(config-if)#switchport	Configure eth2 as a layer 2 port.
SW1(config-if)#bridge-group 1	Associate bridge to an interface.
SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth2 interface.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth3	Enter interface mode.
SW1(config-if)#switchport	Configure eth3 as a layer 2 port.
SW1(config-if)#bridge-group 1	Associate bridge to an interface.
SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#no igmp snooping	Disable IGMP snooping
SW1(config)#exit	Exit configure mode

R1

R1#configure terminal	Enter configure mode.
R1(config)#bridge 1 protocol ieee vlan-bridge	Configure bridge as IEEE VLAN bridge
R1(config)#vlan 2 bridge 1 state enable	Configure VLANs
R1(config)#ip multicast-routing	Configure multicast routing on R1
R1(config)#ip pim rp-address 1.1.1.4	Statically configure RP address for multicast groups.
R1(config)#interface lo	Enter interface mode.
R1(config-if)#ip address 1.1.1.1/32	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#exit	Exit interface mode.
R1(config)#interface eth1	Enter interface mode.
R1(config-if)#switchport	Configure eth3 as a Layer 2 port.
R1(config-if)#bridge-group 1	Associate bridge to an interface.
R1(config-if)#switchport mode trunk	Configure port as a trunk.
R1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface vlan1.2	Enter interface mode.
R1(config-if)#ip address 100.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#ip pim redundancy 1 vrrp dr-priority 101	Configure VRRP aware PIM command with dr-priority and VRRP instance
R1(config)#interface eth2	Enter interface mode.
R1(config-if)#ip address 20.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode

R1(config)#interface eth3	Enter interface mode.
R1(config-if)#ip address 29.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#exit	Exit interface mode.
R1(config)#interface eth4	Enter interface mode.
R1(config-if)#ip address 5.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#exit	Exit interface mode.
R1(config)#router ospf 1	Set the routing process ID.
R1(config-router)#network 1.1.1.1/32 area 0.0.0.0	Configure OSPF network in area 0
R1(config-router)#ospf router-id 1.1.1.1	Configure OSPF router-ID
R1(config-router)#network 20.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0
R1(config-router)#network 29.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0
R1(config-router)#network 5.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0
R1(config-router)#exit	Exit router mode.
R1(config)#router vrrp 1 vlan1.2	Create a VRRP instance for interface VLAN1.2
R1(config-router)#virtual-ip 100.1.1.1	Set the virtual IP address for the VRRP session
R1(config-router)#enable	Enable the VRRP session on the router.

R2

R2#configure terminal	Enter configure mode.
R2(config)#bridge 1 protocol ieee vlan-bridge	Configure bridge as IEEE VLAN bridge
R2(config)#vlan 2 bridge 1 state enable	Configure VLANs
R2(config)#ip multicast-routing	Configure multicast routing on R2
R2(config)#ip pim rp-address 1.1.1.4	Statically configure RP address for multicast groups.
R2(config)#interface lo	Enter interface mode.
R2(config-if)#ip address 1.1.1.2/32	Configure the IP address of the interface.
R2(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R2(config-if)#exit	Exit interface mode.
R2(config)#interface eth1	Enter interface mode.
R2(config-if)#ip address 50.1.1.2/24	Configure the IP address of the interface.
R2(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R2(config)#interface eth2	Enter interface mode.
R2(config-if)#switchport	Configure eth3 as a Layer 2 port.
R2(config-if)#bridge-group 1	Associate bridge to an interface.
R2(config-if)#switchport mode trunk	Configure port as a trunk.

`R2(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`R2(config)#interface eth3`	Enter interface mode.
`R2(config-if)#ip address 29.1.1.2/24`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface vlan1.2`	Enter interface mode.
`R2(config-if)#ip address 100.1.1.2/24`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config-if)#ip pim redundancy 1 vrrp dr-priority 101`	Configure VRRP aware PIM command with dr-priority and VRRP instance
`R2(config)#router ospf 1`	Set the routing process ID .
`R2(config-router)#ospf router-id 1.1.1.2`	Configure OSPF router-ID
`R2(config-router)#network 1.1.1.2/32 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#network 29.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#network 50.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#exit`	Exit router mode.
`R2(config)#router vrrp 1 vlan1.2`	Create a VRRP instance for interface VLAN1.2
`R2(config-router)#virtual-ip 100.1.1.1`	Set the virtual IP address for the VRRP session
`R2(config-router)#enable`	Enable the VRRP session on the router.
`R2(config-router)#exit`	Exit router mode.

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`R3(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`R3(config)#ip multicast-routing`	Configure multicast routing on R3
`R3(config)#ip pim rp-address 1.1.1.4`	Statically configure RP address for multicast groups.
`R3(config)#interface lo`	Enter interface mode.
`R3(config-if)#ip address 1.1.1.3/32`	Configure the IP address of the interface.
`R3(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface eth1`	Enter interface mode.
`R3(config-if)#switchport`	Configure eth3 as a Layer 2 port.
`R3(config-if)#bridge-group 1`	Associate bridge to an interface.
`R3(config-if)#switchport mode trunk`	Configure port as a trunk.
`R3(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`R3(config)#interface eth2`	Enter interface mode.

R3(config-if)#ip address 20.1.1.2/24	Configure the IP address of the interface.
R3(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R3(config)#interface eth3	Enter interface mode.
R3(config-if)#ip address 45.1.1.2/24	Configure the IP address of the interface.
R3(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R3(config-if)#exit	Exit interface mode.
R3(config)#interface vlan1.2	Enter interface mode.
R3(config-if)#ip address 200.1.1.2/24	Configure the IP address of the interface.
R3(config-if)#ip pim sparse-mode	Configure PIM as sparse mode.
R3(config-if)#exit	Exit interface mode.
R3(config)#router ospf 1	Set the routing process ID.
R3(config-router)#ospf router-id 1.1.1.3	Configuring OSPF router-ID.
R3(config-router)#network 1.1.1.3/32 area 0.0.0.0	Configure OSPF network in area 0.
R3(config-router)#network 200.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0.
R3(config-router)#network 20.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0.
R3(config-router)#network 45.1.1.0/24 area 0.0.0.0	Configure OSPF network in area 0.
R3(config-router)#exit	Exit router mode.

R4

R4#configure terminal	Enter configure mode.
R4(config)#bridge 1 protocol ieee vlan-bridge	Configure bridge as IEEE VLAN bridge
R4(config)#vlan 2 bridge 1 state enable	Configure VLANs
R4(config)#ip multicast-routing	Configure multicast routing on R4
R4(config)#ip pim rp-address 1.1.1.4	statically configure RP address for multicast groups.
R4(config)#interface lo	Enter interface mode.
R4(config-if)#ip address 1.1.1.4/32	Configure the IP address of the interface.
R4(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R4(config-if)#exit	Exit interface mode.
R4(config)#interface eth1	Enter interface mode.
R4(config-if)#ip address 50.1.1.1/24	Configure the IP address of the interface.
R4(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R4(config)#interface eth2	Enter interface mode.
R4(config-if)#switchport	Configure eth3 as a Layer 2 port.
R4(config-if)#bridge-group 1	Associate bridge to an interface.
R4(config-if)#switchport mode trunk	Configure port as a trunk.
R4(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.

`R4(config)#interface eth3`	Enter interface mode.
`R4(config-if)#ip address 45.1.1.1/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface eth4`	Enter interface mode.
`R4(config-if)#ip address 5.1.1.2/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface vlan1.2`	Enter interface mode.
`R4(config-if)#ip address 200.1.1.1/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#router ospf 1`	Set the routing process ID .
`R4(config-router)#ospf router-id 1.1.1.4`	Configuring OSPF router-ID
`R4(config-router)#network 1.1.1.4/32 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 200.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 45.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 50.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 5.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#exit`	Exit router mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`SW2(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`SW2(config)#interface eth1`	Enter interface mode.
`SW2(config-if)#switchport`	Configure eth1 as a Layer 2 port.
`SW2(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW2(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW2(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface eth2`	Enter interface mode.
`SW2(config-if)#switchport`	Configure eth2 as a Layer 2 port.
`SW2(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW2(config-if)#switchport mode trunk`	Configure port as a trunk.

SW2(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth2 interface.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth3	Enter interface mode.
SW2(config-if)#switchport	Configure eth3 as a Layer 2 port.
SW2(config-if)#bridge-group 1	Associate bridge to an interface.
SW2(config-if)#switchport mode trunk	Configure port as a trunk.
SW2(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#exit	Exit configure mode

Validation

Verify that PIM DR is the same node as VRRP Master.

Validation 1

```
R1#show  ip ospf  neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface           Instance ID
1.1.1.5           1   Full/DR          00:00:31    5.1.1.2         eth4                  0
1.1.1.3           1   Full/DR          00:00:36    10.2.3.2        eth3                0
1.1.1.4           1   Full/DR          00:00:35    10.2.4.2        eth2                0

R1#show  vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Master
 Virtual IP address: 100.1.1.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 100.1.1.1
 Operational master IP address: 100.1.1.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Master uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE

R1#show  ip pim neighbor
```

```
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
5.1.1.2         eth4                01:55:57/00:01:18         v2    1 / DR
10.2.4.2        eth2               01:45:57/00:01:18         v2    1 / DR
10.2.3.2        eth3               02:13:01/00:01:44         v2    1 / DR
100.1.1.2       vlan1.2            00:01:39/00:01:29         v2    1 /

R1#show  ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 5
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1

(*, 224.1.1.1)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:
Source: 200.1.1.5
 Outgoing  .....o.........................
 KAT timer running, 116 seconds remaining
 Packet count 1

(*, 224.1.1.2)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:

(*, 224.1.1.3)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:
```

```
(*, 224.1.1.4)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:

(*, 224.1.1.5)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:

R1#show  ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(200.1.1.5, 224.1.1.1), uptime 00:01:38, stat expires 00:02:43
Owner PIM, Flags: TF
  Incoming interface: eth4
  Outgoing interface list:
    vlan1.2 (1)
```

Validation 2

```
R2#show  ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
10.2.3.1        eth3                02:13:36/00:01:31         v2    1 /
10.3.5.2        eth1                00:07:45/00:01:30         v2    1 / DR
100.1.1.1       vlan1.2            00:02:14/00:01:36         v2    101 / DR

R2#show  ip pim neighbor detail
Nbr 10.2.3.1 (eth3)
 Expires in 87 seconds, uptime 02:13:40
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 1, Gen ID: 234024133,
 Interface ID: Router-ID: 1.1.1.2 Local-ID: 10030,
```

```
Nbr 10.3.5.2 (eth1), DR
 Expires in 86 seconds, uptime 00:07:49
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 1, Gen ID: 2078598240,
 Interface ID: Router-ID: 1.1.1.5 Local-ID: 10050,

Nbr 100.1.1.1 (vlan1.2), DR
 Expires in 91 seconds, uptime 00:02:18
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 101, Gen ID: 379671611,
 Interface ID: Router-ID: 1.1.1.2 Local-ID: 10066,

R2#show  vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Backup
 Virtual IP address: 100.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 100.1.1.2
 Operational master IP address: 100.1.1.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 1 hours 30 minutes 5 seconds (540500 centi sec)
 Skew time: 60 centi sec
 Master Down Interval: 360 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE
```

Multicast Routing Information Base Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Multicast Commands

OcNOS multicast protocol modules work with the Multicast Routing Information Base (MRIB).

clear ip mroute

Use this command to delete entries from the IP multicast routing table. This command clears the multicast route entries in the multicast route table and removes the entries from the multicast forwarder. MRIB sends a clear message to the multicast protocols. Each multicast protocol has its own clear multicast route command. The protocol-specific clear command clears multicast routes from the protocol and clears the routes from the MRIB.

Command Syntax

```
clear ip mroute *
clear ip mroute A.B.C.D
clear ip mroute A.B.C.D A.B.C.D
clear ip mroute statistics *
clear ip mroute statistics A.B.C.D
clear ip mroute statistics A.B.C.D A.B.C.D
clear ip mroute A.B.C.D pim sparse-mode
clear ip mroute A.B.C.D A.B.C.D pim (dense mode| sparse-mode)
clear ip mroute (vrf NAME|) *
clear ip mroute (vrf NAME|) A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) statistics *
clear ip mroute (vrf NAME|) statistics A.B.C.D
clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D
clear ip mroute (vrf Name|) A.B.C.D pim sparse-mode
clear ip mroute (vrf Name|) A.B.C.D A.B.C.D pim (dense-mode | sparse-mode)
```

Parameters

`*`	All multicast routes.
`A.B.C.D`	Group IP address.
`A.B.C.D`	Source IP address.
`vrf`	VRF name.
`statistics`	Multicast route statistics.
`dense-mode`	Dense Mode (PIM-DM).
`sparse-mode`	sparse Mode (PIM-SM)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip mroute vrf VRF_A 225.1.1.1 3.3.3.3
```

debug ip mrib

Use this command to set debug options for IPv4 multicast.

Use the no parameter with this command to disable debugging IPv4 multicast.

Command Syntax

```
debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
debug ip mrib (vrf NAME|)(all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ip mrib (vrf NAME|) ((all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
```

Parameters

all	Enable all IPv4 multicast debugging.
event	Enable debugging of multicast events.
fib-msg	Enable debugging of multicast FIB messages
mrib-msg	Enable debugging of multicast MRIB messages
mrt	Enable debugging of multicast route
mtrace	Enable debugging of multicast traceroute
mtrace-detail	Enable detailed debugging of multicast traceroute messages
nsm-msg	Enable debugging of multicast NSM messages
register-msg	Enable debugging of multicast PIM Register messages
stats	Enable debugging of multicast statistics.
vif	Enable debugging of multicast interface
vrf	Specify the VRF name

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip mrib all
```

ip multicast route-limit

Use this command to limit the number of multicast routes that can be added to a multicast routing table. It generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Note: The mroute warning threshold must not exceed the mroute limit.

Use the no parameter with this command to disable this configuration.

Command Syntax

```
ip multicast route-limit <1-2147483647>
ip multicast route-limit <1-2147483647> <1-2147483647>
ip multicast (vrf NAME|) route-limit <1-2147483647>
ip multicast (vrf NAME|) route-limit <1-2147483647> <1-2147483647>
no ip multicast route-limit
no ip multicast (vrf NAME|) route-limit
```

Parameters

`vrf`	VRF name
`<1-2147483647>`	Number of routes
`<1-2147483647>`	Threshold at which to generate a warning message

Default

The default limit and threshold value is 2147483647.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip multicast route-limit 34 24
```

ip multicast ttl-threshold

Use this command to configure the time-to-live (TTL) threshold of packets being forwarded out of an interface. Only multicast packets with a TTL value greater than the threshold are forwarded out of the interface.

Use the no parameter with this command to return to the default TTL threshold.

Command Syntax

```
ip multicast ttl-threshold <1-255>
no ip multicast ttl-threshold
```

Parameters

<1-255>	The time-to-live threshold.

Default

The default TTL value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip multicast ttl-threshold 34
```

ip multicast-routing

Use this command to turn on/off multicast routing on the router; when turned off, the multicast protocol daemon remains present, but does not perform multicast functions. When multicast routing is enabled, the MRIB re-creates tunnels, and starts processing any VIF addition/deletion requests, MRT addition/deletion requests, and any multicast forwarding events.

Use the no parameter with this command to disable this function. When the no parameter is used, the MRIB releases all VIFs and tunnels, cleans up MRTs, stops IGMPv2 operation and stops relaying multicast forwarder events to multicast protocols.

Command Syntax

```
ip multicast-routing
ip multicast-routing (vrf NAME|)
no ip multicast-routing
no ip multicast-routing (vrf NAME|)
```

Parameter

vrf	Specify the VRF name.

Default

By default, multicast routing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip multicast-routing
```

ip multicast bidirectional enable

Data Plane may require specific resource allocations for enabling multipoint to multipoint (bidirectional) multicast data forwarding. To configure data plane for such resource allocation use this command.

Prepend no to the same command to revert this configuration.

Command Syntax

```
ip multicast bidirectional enable
no ip multicast bidirectional enable
```

Parameters

None

Default

By default, bidirectional forwarding is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config) # ip multicast bidirectional enable
```

show debugging ip mrib

Use this command to display IPv4 multicast debugging information.

Command Syntax

```
show debugging ip mrib
show debugging ip mrib (vrf NAME|)
```

Parameters

`vrf`	Display routes from a VPN Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output of the `show debugging ip mrib` command.

```
#show debugging ip mrib
Debugging status:
  MRIBv4 event debugging is on
  MRIBv4 VIF debugging is on
  MRIBv4 route debugging is on
  MRIBv4 route statistics debugging is on
  MRIBv4 FIB message debugging is on
  MRIBv4 PIM Register message debugging is on
  MRIBv4 NSM IPC message debugging is on
  MRIBv4 MRIB IPC message debugging is on
  MRIBv4 traceroute debugging is on
  MRIBv4 traceroute detailed debugging is on
#
```

show ip mroute

Use this command to display the IP multicast routing (mroute) table. The routing table is based on the pairing of Source Addresses with their respective Destination Multicast Group Address (S, G).

Command Syntax

```
show ip mroute (dense|sparse|) (count|summary|)
show ip mroute A.B.C.D (dense|sparse|)(count|summary|)
show ip mroute A.B.C.D A.B.C.D (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) A.B.C.D (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) A.B.C.D A.B.C.D (dense|sparse|) (count|summary|)
```

Parameters

`A.B.C.D`	Source or Group IP address.
`count`	Route and packet count data.
`summary`	Provide abbreviated display.
`dense`	Show dense multicast routes.
`sparse`	Show sparse multicast routes.
`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying the IP multicast routing table, with and without specifying the group and source IP address:

```
rtr6#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.0.13), uptime 00:09:39
Owner PIM, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

The following is a sample output of this command displaying the packet count from the IP multicast routing table:

```
#show ip mroute count

IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output for this command displaying the IP multicast routing table in an abbreviated form:

```
#show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.0.13), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

The following is a sample output for this command displaying the IP multicast routing table for Bidirectional routes:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(*, 225.0.0.0)/24, uptime 00:01:53
Owner PIM, Flags: FB
RPA ID: 4
Outgoing interface list:
vlan1.10 (1)

(*, 225.0.0.1)/32, uptime 00:00:20
Owner PIM, Flags: FB
RPA ID: 4
Outgoing interface list:
vlan1.10 (1)
vlan1.20 (1)
```

Table 1-25: Mroute pointers

Pointers	Description
I	Immediate statistics
T	Timed statistics
F	Forwarder installed
B	Bidirectional
Timers	• Uptime – route uptime. • Statistics Expiry –The time the routing table waits before updating statistics.
Interface State	Interface Time to Live (TTL)

Table 1-26: Show ip mroute output

Entry	Description
(a.d.c.d, 224.x.x.x)	Source Address paired with its Destination Multicast Group Address
uptime	As stated.
Owner	The owner is derived from the multicast group notable address (IANA). In the example above, the owner is specified as PIM because it is using the IANA address: 224.0.0.13. Other owners can be OSPF (224.0.0.5), IS-IS (224.0.0.19–21), and so on.
Flags	The flags associated with this mroute table entry.
Incoming interface	The name of the in coming interface (eth1, xe5/2, etc.).
Outgoing interface list	A numbered list of the outgoing interfaces

Table 1-27: Show ip mroute statistics received and sent

Entry	Description
NOCACHE	Number of No Cache messages received.
WRONGVIF	The Virtual Host Interface (VIF) enables the router to send and receive IP multicast packets on several different interfaces at once. This is the count of wrong VIFs received.
WHOLEPKT	When a source is multicasting a large volume data and the PIM router does not know about the particular Rendezvous Point (RP(G)), the PIM process will constantly receive WHOLEPKT notification from the kernel – this shows the count of such notifications.

show ip mvif

Use this command to display the MRIB VIF table entries.

The Virtual Host Interface (VIF) used in Pragmatic General Multicast (PGM) or “Reliable Multicast.” The VIF enables the router to send and receive IP multicast packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

Command Syntax

```
show ip mvif
show ip mvif IFNAME
show ip mvif (vrf NAME|)
show ip mvif (vrf NAME|) IFNAME
```

Parameters

IFNAME	Specify the interface name.
vrf	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following are sample outputs of this command displaying the contents for the MRIB VIF table, both with and without the interface parameter specified:

```
#show ip mvif
Interface    Vif   Owner    TTL  Local            Remote           Uptime
             Idx   Module        Address          Address
wm0          0     PIM-SM   1    192.168.1.53     0.0.0.0          00:04:26
Register     1               1    192.168.1.53     0.0.0.0          00:04:26
wm1          2     PIM-SM   1    192.168.10.53    0.0.0.0          00:04:25
#show ip mvif wm0
Interface   Vif   Owner    TTL  Local            Remote           Uptime
            Idx   Module        Address          Address
wm0         0     PIM-SM   1    192.168.1.53     0.0.0.0          00:05:17
```

Table 1-28: Show ip mvif output

Entries	Description
Interface	The name of the interface.
Vif Idx	The VIF Index – the numbering of the entries in the MRIB table.
Owner	What multicast protocol is being used for an entry. For example, PIM-SM (PIM Sparce Mode).

Table 1-28: Show ip mvif output (Continued)

Entries	Description
TTL	Time to Live for the entry.
Local Address	AS stated.
Remote Address	As stated.
Uptime	How long the multicast interface has been operating.

show ip multicast rpa

Bidirectional (multipoint to multipoint) multicast forwarding uses a list of incoming interfaces. These interface list is created for each bidirectional RP. Such an entity is identified with an id number. When a bidirectional route object is programmed, this id would be used to indicate it'sits incoming interface list. This command outputs this entity list. Use this command to display the MRIB rpa details.

Command Syntax

show ip multicast rpa

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in before OcNOS version 4.0.

Example

```
#show ip multicast rpa

IP Multicast bidir rpa
2.2.2.2:1 uptime 00:23:16
  Incoming interface list:
      vlan1.50 (3)
      vlan1.30 (0)
      vlan1.40 (2)
```

snmp restart mribd

Use this command to restart SNMP in Multicast Routing Information Base (MRIB)

Command Syntax

```
snmp restart mribd
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart mribd
```

CHAPTER 2 Layer 3 IGMP Multicast Commands

This chapter describes the commands for Internet Group Management Protocol (IGMP) including the IGMP proxy service.

For IGMP multicast snooping commands, see Chapter 3, *Layer 2 IGMP Snooping Multicast Commands*.

clear ip igmp

Use this command to clear all IGMP local-memberships on all interfaces. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, or IGMP Proxy.

Command Syntax

```
clear ip igmp
clear ip igmp group *
clear ip igmp group A.B.C.D
clear ip igmp group A.B.C.D IFNAME
clear ip igmp interface IFNAME
clear ip igmp (vrf NAME|)
clear ip igmp (vrf NAME|) group *
clear ip igmp (vrf NAME|) group A.B.C.D
clear ip igmp (vrf NAME|) group A.B.C.D IFNAME
clear ip igmp (vrf NAME|) interface IFNAME
```

Parameters

`*`	Clears all groups on all interfaces.
`A.B.C.D`	Specify the group address's local-membership to be cleared from all interfaces.
`interface`	Specify an interface. All groups learned from this interface are deleted.
`IFNAME`	Specify name of the interface.
`vrf`	Specify the VRF name.
`group`	Deletes IGMP group cache entries.
`interface`	Specify name of the interface; all groups learned from this interface are deleted.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip igmp
#clear ip igmp group *
#clear ip igmp group 224.1.1.1
#clear ip igmp interface eth1
#clear ip igmp vrf VRF_A
#clear ip igmp vrf new group *
#clear ip igmp vrf new interface eth1
```

debug ip igmp

Use this command to enable debugging of all IGMP, or a specific component of IGMP. This command applies to interfaces configured for IGMP Layer-3 multicast protocols.

Use the no parameter with this command to disable all IGMP debugging, or select a specific IGMP component.

Command Syntax

```
debug ip igmp all
debug ip igmp decode
debug ip igmp encode
debug ip igmp events
debug ip igmp fsm
debug ip igmp tib
debug ip igmp (vrf NAME|) all
debug ip igmp (vrf NAME|) decode
debug ip igmp (vrf NAME|) encode
debug ip igmp (vrf NAME|) events
debug ip igmp (vrf NAME|) fsm
debug ip igmp (vrf NAME|) tib
no debug ip igmp all
no debug ip igmp decode
no debug ip igmp encode
no debug ip igmp events
no debug ip igmp fsm
no debug ip igmp tib
no debug ip igmp (vrf NAME|) all
no debug ip igmp (vrf NAME|) decode
no debug ip igmp (vrf NAME|) encode
no debug ip igmp (vrf NAME|) events
no debug ip igmp (vrf NAME|) fsm
no debug ip igmp (vrf NAME|) tib
```

Parameters

`all`	Debug all IGMP.
`decode`	Debug IGMP decoding.
`encode`	Debug IGMP encoding.
`events`	Debug IGMP events.
`fsm`	Debug IGMP Finite State Machine (FSM).
`tib`	Debug IGMP Tree Information Base (TIB).

`vrf`	Debug VPN Routing/Forwarding instance.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip igmp all
```

ip igmp

Use this command to enable the IGMP operation on an interface. This command enables IGMP operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface. This command will has no effect on interfaces configured for IGMP proxy.

Use the no parameter with this command to return all IGMP related configuration to the default (including IGMP proxy service).

Command Syntax

```
ip igmp
no ip igmp
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp
```

ip igmp access-group

Use this command to control the multicast local-membership groups learned on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP proxy.

Use the no parameter with this command to disable this access control.

Command Syntax

```
ip igmp access-group WORD
no ip igmp access-group WORD
```

Parameters

WORD	Standard IP access-list name.

Default

No access list configured

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can only join the group 225.2.2.2:

```
#configure terminal
(config)#access-list 1 permit 225.2.2.2 0.0.0.0
(config)#interface eth1
(config-if)#ip igmp access-group xyz
(config-if)#exit
```

ip igmp immediate-leave

In IGMP version 2, use this command to minimize the leave latency of IGMP memberships. This command is used when only one receiver host is connected to each interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP Proxy.

To disable this feature, use the no parameter with this command.

Command Syntax

```
ip igmp immediate-leave group-list WORD
no ip igmp immediate-leave
```

Parameters

group-list	Standard access-list name or number that defines multicast groups in which the immediate leave feature is enabled.
WORD	Standard IP access-list name.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one host membership at a time per interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp immediate-leave group-list xyz
(config-if)#exit
(config)#access-list 34 permit 225.192.20.0 0.0.0.255
```

ip igmp join-group

Use this command to configure a join multicast group.

Use the no parameter with this command to delete group membership entry.

Command Syntax

```
ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}
no ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}
```

Parameters

A.B.C.D	Standard IP multicast group address to be configured as a group member.
source	Static source to be joined.
A.B.C.D	Standard IP source address to be configured as a source from where multicast packets originate.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp join-group 225.1.1.1 source 1.1.1.2

(config-if)#no ip igmp join-group 225.1.1.1 source 1.1.1.2
```

ip igmp last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the no parameter with this command to return to the default value on an interface.

Command Syntax

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

Parameter

<2-7>	Specify the last member query count value.

Default

The default last member query count value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-count 3
```

ip igmp last-member-query-interval

Use this command to configure the frequency at which the router sends IGMP group-specific host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the no parameter with this command to set this frequency to the default value.

Command Syntax

```
ip igmp last-member-query-interval <1000-25500>
no ip igmp last-member-query-interval
```

Parameter

<1000-25500>	Frequency (in milliseconds) at which IGMP group-specific host query messages are sent.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the IGMP group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-interval 2000
```

ip igmp limit

Use this command to set the maximum number of group membership states, at either the router level or at the interface level. Once the specified number of group memberships is reached, all further local-memberships are ignored. Optionally, an exception access-list can be configured to specify the group-address(es) to be excluded from being subject to the limit.

This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. The limit applies, individually, to each of its constituent interfaces.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax

```
ip igmp limit (<1-2097152> (except WORD |)
ip igmp (vrf NAME) limit(<1-2097152> (except WORD |)
no ip igmp limit
no ip igmp (vrf NAME|) limit
```

Parameters

`vrf`	Specify the VRF name.
`<1-2097152>`	Maximum number of group membership states.
`except`	Number or name that defines multicast groups that are exempted from being subject to configured limit.
`WORD`	Standard IP access-list name.

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures an IGMP limit of 100 group-membership states across all interfaces on which IGMP is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
(config)#access-list 1 permit 224.1.1.1 0.0.0.0
(config)#ip igmp limit 100 except xyz
```

The following example configures an IGMP limit of 100 group-membership states on eth1:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp limit 100
```

ip igmp mroute-proxy

Use this command to specify the IGMP Proxy service (upstream host-side) interface with which to be associated. IGMP router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast routing protocol, otherwise the behavior will be undefined.

Use the no parameter with this command to remove the association with the proxy-service interface.

Command Syntax

```
ip igmp mroute-proxy IFNAME
no ip igmp mroute-proxy
```

Parameter

IFNAME	Specify an interface name.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the eth1 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp mroute-proxy eth1
```

ip igmp offlink

Use this command to configure off-link for IGMP.

Use the no parameter with this command to remove this configuration.

Command Syntax

```
ip igmp offlink
no ip igmp offlink
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp offlink

(config-if)#no ip igmp offlink
```

ip igmp proxy-service

Use this command to designate an interface to be the IGMP proxy-service (upstream host-side) interface, thus enabling IGMP host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to IGMP host-side functionality.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast-routing protocol, otherwise the behavior will be undefined.

Use the no parameter with this command to remove the designation of the interface as an upstream proxy-service interface.

Command Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example designates the eth1 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy-service
```

ip igmp proxy unsolicited-report-interval

Use this command to set an unsolicited report interval for an interface designated as an IGMP proxy (upstream host-side).

Use the no parameter with this command to remove the unsolicited report interval from the interface.

Command Syntax

```
ip igmp proxy unsolicited-report-interval <1000-25500>
no ip igmp proxy unsolicited-report-interval
```

Parameter

<1000-25500>	Specify an unsolicited report interval value in milliseconds.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy unsolicited-report-interval 1234

(config-if)#no ip igmp proxy unsolicited-report-interval
```

ip igmp querier-timeout

Use this command to set the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To restore the default value, use the no parameter with this command.

Command Syntax

```
ip igmp querier-timeout <60-300>
no ip igmp querier-timeout
```

Parameter

<60-300>	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier.

Default

255 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp querier-timeout 120
```

ip igmp query-interval

Use this command to set the frequency of sending IGMP host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default frequency, use the no parameter with this command.

Note: Querier timeout changes by changing query interval.

Command Syntax

```
ip igmp query-interval <1-18000>
no ip igmp query-interval
```

Parameter

<1-18000>	Frequency (in seconds) at which IGMP host query messages are sent.

Default

Default query interval is 125 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the frequency of sending IGMP host-query messages to 2 minutes:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-interval 120
```

ip igmp query-max-response-time

Use this command to set the maximum response time advertised in IGMP queries. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the no parameter with this command to restore the default value.

Command Syntax

```
ip igmp query-max-response-time <1-240>
no ip igmp query-max-response-time
```

Parameter

<1-240>	Maximum response time (in seconds) advertised in IGMP queries.

Default

10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-max-response-time 8
```

ip igmp ra-option

Use this command to configure strict RA (Router Advertisement) validation for IGMP.

Use the no parameter with this command to restore the default value.

Command Syntax

```
ip igmp ra-option
no ip igmp ra-option
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp ra-option

(config-if)#no ip igmp ra-option
```

ip igmp robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default value on an interface, use the no parameter with this command.

Command Syntax

```
ip igmp robustness-variable <2-7>
no ip igmp robustness-variable
```

Parameter

<2-7>	Specify the robustness variable value.

Default

Default robustness variable value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp robustness-variable 3
```

ip igmp ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax

```
ip igmp ssm-map enable
ip igmp (vrf NAME|) ssm-map enable
no ip igmp ssm-map enable
no ip igmp (vrf NAME|) ssm-map enable
```

Parameter

`vrf`	Specify the VRF name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to configure SSM mapping on the router.

```
#configure terminal
(config)#ip igmp ssm-map enable
```

ip igmp ssm-map static

Use this command to specify the static mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to remove the SSM map association.

Command Syntax

```
ip igmp ssm-map static WORD A.B.C.D
ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D
no ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D
no ip igmp ssm-map static WORD A.B.C.D
```

Parameters

`vrf`	Specify the VRF name.
`WORD`	Standard IP access-list name.
`A.B.C.D`	Source address to use for static map group.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to configure an SSM static mapping for group-address 224.1.1.1

Note: `access-list` can only be a `permit` type `access-list`

```
#configure terminal
(config)# ip igmp ssm-map static xyz 1.2.3.4
(config)# access-list 1 permit 224.1.1.1 0.0.0.255
```

ip igmp static-group

Use this command to statically configure group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to IGMP operation on a specific interface to statically add group and/or source records; on a VLAN interface to statically add group and/or source records.

Use the no parameter with this command to delete static group membership entries.

Command Syntax

```
ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
no ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
```

Parameters

A.B.C.D	Standard IP Multicast group address to be configured as a static group member.
source	Static source to be joined.
A.B.C.D	Standard IP source address to be configured as a static source from where multicast packets originate.
ssm-map	Mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate these (*, G) groups' memberships to (S, G) memberships for use with PIM-SSM.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show how to statically add group and/or source records for IGMP:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.3

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.4 source 1.2.3.4

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.5 source ssm-map
```

ip igmp startup-query-count

Use this command to set a startup query count for IGMP.

Use the no parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-count <2-10>
no ip igmp startup-query-count
```

Parameters

<2-10>	Specify a startup query count value.

Default

The default value 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-count 2

(config-if)#no ip igmp startup-query-count
```

ip igmp startup-query-interval

Use this command to set a query interval value for IGMP.

Use the no parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-interval <1-18000>
no ip igmp startup-query-interval
```

Parameters

<1-18000>	Specify a startup query interval value in seconds.

Default

The default value 31 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-interval 1

(config-if)#no ip igmp startup-query-interval
```

ip igmp version

Use this command to set the current IGMP protocol version on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the no parameter with this command to return to the default version.

Command Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameters

<1-3>	Specify IGMP protocol version number.

Default

The default IGMP protocol version number is 3.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp version 2
```

show debugging ip igmp

Use this command to display the status of the debugging of the IGMP system, or a specific VRF in the IGMP system.

Command Syntax

```
show debugging ip igmp
show debugging ip igmp (vrf NAME|)
```

Parameters

`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ip igmp
 IGMP Debugging status:
 IGMP Decoder debugging is on
 IGMP Encoder debugging is on
 IGMP Events debugging is on
 IGMP FSM debugging is on
 IGMP Tree-Info-Base (TIB) debugging is on
```

show ip igmp groups

Use this command to display the multicast groups with receivers connected to the router and learned through IGMP.

Command Syntax

```
show ip igmp groups (detail|)
show ip igmp groups A.B.C.D (detail|)
show ip igmp groups IFNAME (detail|)
show ip igmp groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups (detail|)
show ip igmp (vrf NAME|) groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups IFNAME (detail|)
show ip igmp (vrf NAME|) groups IFNAME A.B.C.D (detail|)
```

Parameters

`vrf`	Specify the VRF name.
`A.B.C.D`	Address of multicast group.
`IFNAME`	Name of the interface.
`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following command displays local-membership information for all interfaces:

```
rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface:      eth1
Group:          224.1.1.1
Flags:          L
Uptime:         00:00:04
Group mode:     Exclude (Expires: 00:04:15, Static)
Last reporter:   3.3.3.3
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)
Include Source List :
 Source Address Uptime    v3 Exp    Fwd Flags
 2.2.2.2         00:00:04 stopped   Yes L
```

Table 2-29 shows the flags codes displayed at the start of a group entry.

Table 2-29: Flags

Flag	Meaning
M	Source Specific Multicast
R	Remote multicast
L	Local multicast
SG	Static Group
SS	Static Source

Table 2-30 explains the output fields.

Table 2-30: show ip igmp groups output

Entry	Description
Interface	The interface on which multicast is operating.
Group	The Multicast group, identified by a multicast IP address.
Flags	Flag on this interface – in this case, the flag indicates that the multicast is Local. See Table 2-29.
Uptime	The amount of time that the multicast connection has been up.
Group mode	The group mode is determined by interactions between IGMP router database entries, which is beyond the scope of this document. For a detailed description of these interactions, see RFC 3376.
Last reporter	The IPv4 address of the last host to send multicast information.
Group source list	A list of flags that indicate the state of the multicast connections. See Table 2-29.
Include Source List	A table containing parameters about the multicast session: • Source Address – The IP address of the Source(s) connected to the multicast hosts. • Uptime – The multicast session's uptime. • v3 Exp – Tells whether IGMPv3 Explicit Tracking is running or not. • Fwd – Whether IGMP information is being forwarded by this device. • Flags – See Table 2-29.

show ip igmp interface

Use this command to display the state of IGMP, IGMP Proxy service for a specified interface, or all interfaces.

Command Syntax

```
show ip igmp interface (IFNAME|)
show ip igmp (vrf NAME|) interface (IFNAME|)
```

Parameters

`vrf`	Specify the VRF name.
`interface`	Specify the interface parameter.
`IFNAME`	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the IGMP interface status on all interfaces enabled for IGMP.

```
#show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds|
#
```

Table 2-31 explains the output fields.

Table 2-31: show ip igmp interface

Entry	Description
Interface	Interface type and number
IGMP Active	IGMP status – whether Active or Inactive; whether this interface is a querier; IGMP version (v1, v2, or v3).
IGMP querying router	IP address of the designated router for this LAN segment.
IGMP query interval	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages.
IGMP querier timeout	An interval of time that the software uses when deciding to take over as the querier.

Table 2-31: show ip igmp interface (Continued)

Entry	Description
IGMP max query response time	An interval of time that is advertised as the maximum response time that is advertised in IGMP queries.
Last member query response interval	This interval is the maximum amount of time between query messages that the querier will wait before sending messages that indicate that the multicast session has ended.
Group Membership interval	A group membership interval timer is maintained for each dynamic multicast group added to a downstream interface in the table. The timer is refreshed when a membership report for a multicast group is received. If the timer expires, the multicast group is removed from the table.

show ip igmp proxy

Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

Command Syntax

```
show ip igmp proxy groups (detail|)
show ip igmp proxy groups A.B.C.D (detail|)
show ip igmp proxy groups IFNAME (detail|)
show ip igmp proxy groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups (detail|)
show ip igmp (vrf NAME|) proxy groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME A.B.C.D (detail|)
```

Parameters

`vrf`	Specify the VRF name.
`groups`	IGMP proxy group membership information.
`A.B.C.D`	Address of multicast group.
`IFNAME`	The name of the VLAN interface.
`detail`	IGMPv3 source information

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1

#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```

Table 2-32 explains the output fields.

Table 2-32: show ip igmp proxy output

Entry	Description
Interface	Interface and Index of the interface.
Administrative status	Depends on the interface states – Enabled only if both host and downstream interfaces are up. Otherwise, Disabled if only one interface is up.
Operational status	Depends on Administrative status – either Up or Down depending on Administrative status of corresponding interfaces.
Upstream interface	As stated.
Number of multicast groups	The number of multicast groups supported by this proxy.

Table 2-33 explains the output fields.

Table 2-33: show ip igmp proxy groups output

Entry	Description
Group Address	Multicast address associated with each group.
Interface	Interface name, such as eth1, xe3/1, etc..
State	The state of the proxy group – can be either Active or Inactive.
Member state	The state of the proxy group member – can be either Idle or Delay, Idle is the default state.

show ip igmp ssm-map

Use this command to display IGMP SSM-map data.

Command Syntax

```
show ip igmp ssm-map
show ip igmp ssm-map A.B.C.D
show ip igmp (vrf NAME|) ssm-map
show ip igmp (vrf NAME|) ssm-map A.B.C.D
```

Parameters

`vrf`	Specify the VRF name.
`A.B.C.D`	Address of multicast group.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ip igmp ssm-map
SSM Mapping : Enabled
Database    : Static mappings configured
```

CHAPTER 3 Layer 2 IGMP Snooping Multicast Commands

This chapter describes commands for Internet Group Management Protocol (IGMP) multicast snooping.

igmp snooping

Use this command to enable IGMP Snooping. When this command is given in the Configure mode, IGMP snooping is enabled at switch level on all the vlans in switch. When this command is given at the VLAN interface level, IGMP Snooping is enabled for that VLAN.

Note: IGMP Snooping can be only enabled/disabled on VLAN interfaces.

Use the no parameter with this command to globally disable IGMP Snooping, or for the specified interface.

Command Syntax

```
igmp snooping
no igmp snooping
```

Parameter

None

Default

IGMP Snooping is enabled.

Command Mode

Interface mode for VLAN interface

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#igmp snooping
(config)#interface vlan1.1
(config-if)#igmp snooping
```

igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the IGMP group-membership is removed as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the no parameter with this command to disable fast-leave processing.

Command Syntax

```
igmp snooping fast-leave
no igmp snooping fast-leave
```

Parameters

None

Default

IGMP Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable fast-leave processing on a VLAN.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping fast-leave
```

igmp snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the no parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax

```
igmp snooping mrouter interface IFNAME
no igmp snooping mrouter interface IFNAME
```

Parameter

IFNAME	Specify the name of the interface.

Default

IGMP Snooping mrouter processing is disabled.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows interface fe8 statically configured to be a multicast router interface.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping mrouter interface fe8
```

igmp snooping querier

Use this command to enable IGMP snooping querier functionality on a VLAN when IGMP is not enabled on the particular VLAN. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

The IGMP Snooping querier uses the 0.0.0.0 source IP address, because it only masquerades as a proxy IGMP querier for faster network convergence. It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router. It restarts as the IGMP Snooping querier if no queries are seen within the other querier interval.

Use the `no` parameter with this command to disable IGMP querier configuration.

Command Syntax

```
igmp snooping querier
no igmp snooping querier
```

Default

By default, Querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping querier
```

igmp snooping report-suppression

Use this command to enable report suppression for IGMP version 1, 2 and 3 reports.

Use the no parameter with this command to disable report suppression.

Note: IGMP snooping report suppression is not supported on Qumran devices.

Command Syntax

```
igmp snooping report-suppression
no igmp snooping report-suppression
```

Default

By default, report suppression is enabled on x86.

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping report-suppression
```

igmp snooping static-group

Use this command to statically configure group membership entries on an interface

Use the no parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping static-group A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D interface IFNAME
igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.
A.B.C.D	Specify the IP address In case of static-group, Multicast Address to be Joined. In case of source, Source Address to be Joined.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#conf t
(config)#interface vlan1.1
(config-if)#igmp snooping static-group 230.0.0.1 interface xe2
(config-if)#igmp snooping static-group 230.0.0.1 source 10.10.10.10 interface
xe1
(config-if)#exit
(config)#exit
```

show igmp snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax

```
show igmp snooping interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Default

By default, report suppression is disabled on Qumran devices.

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces.

```
#show igmp snooping interface
Global IGMP Snooping information
IGMP Snooping Enabled
IGMPv1/v2 Report suppression Enabled
IGMPv3 Report suppression Enabled
IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
xe5/1
IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds

IGMP Snooping information for vlan1.2
```



```
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds
IGMP Snooping maximum query response time is 10 seconds
IGMP Snooping Startup query interval is 31 seconds
Querier robustness: 2
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
xe5/1
```

show igmp snooping groups

Use this command to display the multicast groups learnt through snooping or statically configured.

Command Syntax

```
show igmp snooping groups
show igmp snooping groups details
show igmp snooping groups A.B.C.D
show igmp snooping groups A.B.C.D detail
show igmp snooping groups IFNAME
show igmp snooping groups IFNAME A.B.C.D
show igmp snooping groups IFNAME A.B.C.D detail
show igmp snooping groups IFNAME detail
```

Parameters

A.B.C.D	Specify multicast group address.
IFNAME	Specify the name of the interface.
detail	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
      #show igmp snooping groups
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200   230.0.0.1             xe1          S     00:02:07   static   0.0.0.0
V3
      #show igmp snooping groups detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:08
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty

      #show igmp snooping groups 230.0.0.1
```

```
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:35   static   0.0.0.0
V3
      #show igmp snooping groups 230.0.0.1 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:37
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty

      #show igmp snooping groups vlan1.200
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:47   static   0.0.0.0
V3
      #show igmp snooping groups vlan1.200 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:50
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty
```

Table 3-34: Show igmp snooping groups

Entries	Description
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Group	The multicast group identified by an IPv4 address.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Group mode	As stated.

Table 3-34: Show igmp snooping groups (Continued)

Entries	Description
Last reporter	In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in group multicast traffic only from those sources in the source address list. If host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source except the sources in the source address list. A host can also send an EXCLUDE report in which the source-list parameter is empty, which is known as an EXCLUDE NULL report. An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources.
Vlan	VLAN number ID.
Group/Source Address	Multicast group and source addresses.
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Expires	Either by a timeout (IGMPv1) or by checking whether the member is still a part of the multicast (IGMPv2 or v3). Can also be statically configured.
Last Reporter	Indicates that the host wants to join a particular multicast group.
Version	IGMP version (v1, v2, or v3).

show igmp snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax

```
show igmp snooping mrouter IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#show igmp snooping mrouter vlan1.1
VLAN    Interface             IP-address    Expires
1         xe1(static)
```

show igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

Command Syntax

```
show igmp snooping statistics interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show igmp snooping statistics interface vlan1.1
IGMP Snooping statistics for vlan1.1
Group Count            :  1
IGMPv1 reports received  :  0
IGMPv2 reports received   :  0
IGMPv2 leaves received   :  0
IGMPv3 reports received   :  0
IGMPv1 query warnings  :  0
IGMPv2 query warnings  :  0
IGMPv3 query warnings  :  0
```

CHAPTER 4 Layer 2 MLD Snooping Commands

This chapter describes the Layer 2 Multicast Listener Discovery (MLD) Snooping commands:

clear mld snooping group

Use this command to clear mld snooping groups.

Command Syntax

```
clear mld snooping group *
clear mld snooping group X.X.X.X (IFNAME|)
```

Parameters

*	Displays all groups
IFNAME	The name of the VLAN interface
X:X::X:X	Source address to use for static map group

Default

By default, mld snooping report suppression is disabled on Qumran devices.

Report suppression does not apply to MLDv2, so it is turned off by default for MLDv1 reports.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear mld snooping group *
```

mld snooping

Use this command to enable MLD snooping. When this command is given in configure mode, MLD snooping is enabled at the switch level. When this command is given at the VLAN interface level, MLD snooping is enabled for that VLAN.

Use the no parameter with this command to globally disable MLD Snooping, or for the specified interface.

Command Syntax

```
mld snooping
no mld snooping
```

Parameters

None

Default

By default, MLD Snooping is enabled.

Command Mode

Configure mode and Interface mode for VLAN interface.

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

The following example shows the setting of accept-lifetime for key1 on the key chain named mychain.

```
#configure terminal
(config)#mld snooping
(config)#interface vlan1.100
(config-if)#mld snooping
```

mld snooping fast-leave

Use this command to enable MLD snooping fast-leave processing. MLD group-membership is removed, as soon as an MLD leave group message is received without sending out a group-specific query.

Use the no parameter with this command to disable fast-leave processing.

Command Syntax

```
mld snooping fast-leave
no mld snooping fast-leave
```

Parameters

None

Default

By default, MLD Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping fast-leave
(config-if)#exit
```

mld snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for MLD snooping in that VLAN.

Use the no parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax

```
mld snooping mrouter interface IFNAME
no mld snooping mrouter interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Default

N/A

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping mrouter interface eth1
(config-if)#exit
```

mld snooping querier

Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

The MLD snooping querier uses the 0.0.0.0 source IP address, because it masquerades as a proxy MLD querier for faster network convergence. It does not start or automatically cease the MLD querier operation if it detects a query message from a multicast router. It restarts as MLD snooping querier if no queries are seen within another querier interval.

Note: This command can only be configured on VLAN interfaces.

Use the no parameter with this command to disable MLD querier configuration.

Command Syntax

```
mld snooping querier
no mld snooping querier
```

Parameters

None

Default

By default, MLD snooping querier is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping querier
(config-if)#exit
```

mld snooping report-suppression

Use this command to enable report suppression for MLD version 1.

Use the no parameter to disable report suppression.

Note: MLD Snooping command can only be configured on VLAN interfaces. MLD snooping report suppression is supported on x86 and not supported on Qumran devices.

Command Syntax

```
mld snooping report-suppression
no mld snooping report-suppression
```

Parameters

None

Default

By default, MLD snooping report suppression is enabled on x86.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping report-suppression
(config-if)#exit
```

show debugging mld snooping

Use this command to display debugging information for MLD.

Command Syntax

```
show debugging mld snooping
```

Parameters

None

Default

N/A

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#show debugging mld snooping
MLD Snooping Debugging status:
  MLD Snooping Decoder debugging is on
  MLD Snooping Encoder debugging is on
  MLD Snooping Events debugging is on
  MLD Snooping FSM debugging is on
  MLD Snooping Tree-Info-Base (TIB) debugging is on
```

show mld snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax

```
show mld snooping mrouter (IFNAME|)
```

Parameters

IFNAME	The name of the VLAN interface

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#show mld snooping mrouter vlan1.100
VLAN      Interface       IP-address                  Expires
100       eth3(dynamic)   fe80::a00:27ff:fe6f:5bc1   00:02:16

#show mld snooping mrouter
VLAN      Interface         IP-address                      Expires
400       eth4(static)      --                              --
100       eth1(dynamic)     fe80::a00:27ff:fe27:9856        00:02:19
200       eth2(dynamic)     fe80::a00:27ff:fe32:7951        00:02:45
300       eth3(dynamic)     fe80::a00:27ff:feff:f063        00:01:51
```

show mld snooping statistics

Use this command to display MLD snooping statistics data.

Command Syntax

```
show mld snooping statistics
show mld snooping statistics (interface IFNAME|)
show mld snooping statistics (count)
```

Parameters

IFNAME	The name of the VLAN interface
Count	Consolidated group statistics

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show mld snooping statistics
MLD Snooping statistics for vlan1.300
 Group Count            :  2
 MLDv1 reports received :  0
 MLDv2 reports received :  2
 MLDv1 leaves received  :  0
 MLDv1 query warnings   :  0
 MLDv2 query warnings   :  0

#show mld snooping statistics count
MLD Snooping consolidated statistics
Total number of groups              :  2
Total MLDv1 reports received        :  0
Total MLDv2 reports received        :  4
Total MLDv1 leaves received         :  2
Total MLDv1 query warnings          :  0
Total MLDv2 query warnings          :  0

#show mld snooping statistics interface vlan1.100
MLD Snooping statistics for vlan1.100
 Group Count                          :  0
 MLDv1 reports received               :  0
 MLDv2 reports received               :  2
 MLDv1 leaves received                :  1
 MLDv1 query warnings                 :  0
 MLDv2 query warnings                 :  0
```

show mld snooping groups

Use this command to display MLD snooping groups.

Command Syntax

```
show mld snooping groups
show mld snooping groups (IFNAME|)
show mld snooping groups (IFNAME|) detail
show mld snooping groups X.X.X.X
show mld snooping groups X.X.X.X detail.
```

Parameters

`IFNAME`	The name of the VLAN interface
`X:X::X:X`	Address of multicast group
`detail`	MLDv2 source information

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh mld snooping groups detail
MLD Connected Group Membership Details for eth3
Interface:      eth3
Group:          ff1e::10
Uptime:         00:00:10
Group mode:     Include ()
Last reporter:  fe80::a00:27ff:febb:5235
Group source list: (R - Remote, M - SSM Mapping, S - Static )
Source Address   Uptime             v2 Exp       Fwd    Flags
3000::10         00:00:10           00:04:09   Yes       R
```

show mld snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax

```
show mld snooping interface (IFNAME|)
```

Parameters

IFNAME	Name of the interface.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh mld snooping interface vlan1.100
 MLD Snooping information for vlan1.100 (Index 9)
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Active, Non-Querier,
 Internet address is fe80::a00:27ff:fe8d:e47a
 MLD querying router is :
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is not enabled
 MLD Snooping report suppression is disabled
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 0
 Active Ports:
  eth2
```

Protocol Independent Multicasting Command Reference

Contents

This document contains these chapters:

CHAPTER 1 PIMv4 Commands

The chapter includes the commands that support the Protocol-Independent Multicast (PIM).

- ip pim propagation-delay
- ip pim register-rate-limit
- ip pim register-rp-reachability
- ip pim register-source
- ip pim register-suppression
- ip pim router-id
- ip pim rp-address
- ip pim rp-candidate
- ip pim rp-register-kat
- ip pim spt-threshold
- ip pim ssm
- ip pim state-refresh origination-interval
- ip pim unicast-bsm
- show debugging ip pim
- show debugging pim
- show ip msdp peer
- show ip msdp sa-cache
- show ip pim interface
- show ip pim interface df
- show ip pim mroute
- show ip pim neighbor
- show ip pim nexthop
- show ip pim bsr-router
- show ip pim local-members
- show ip pim rp-hash
- show ip pim rp mapping
- snmp restart pim
- undebug all ip pim

clear ip mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax

```
clear ip mroute *
clear ip mroute * pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D
clear ip mroute A.B.C.D A.B.C.D
clear ip mroute A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D pim sparse-mode
clear ip mroute statistics *
clear ip mroute statistics A.B.C.D
clear ip mroute statistics A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) *
clear ip mroute (vrf NAME|) * pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D pim sparse-mode
clear ip mroute (vrf NAME|) statistics *
clear ip mroute (vrf NAME|) statistics A.B.C.D
clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`*`	Delete all multicast routes
`pim`	Protocol Independent Multicast (PIM)
`A.B.C.D`	Clears group IP address
`A.B.C.D`	Clears source IP address
`dense-mode`	Clears multicast rout table for PIM dense-mode
`sparse-mode`	Clears multicast route table for PIM sparse mode
`statistics`	Clears multicast route statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip mroute * pim sparse-mode
#clear ip mroute 224.2.2.2 4.4.4.4 pim sparse-mode
```

clear ip msdp peer

Use this command to clear the TCP connection to a Multicast Source Discovery Protocol (MSDP) peer.

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Command Syntax

```
clear ip msdp peer (A.B.C.D|)
clear ip msdp (vrf NAME|) peer (A.B.C.D|)
```

Parameters

A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#clear ip msdp peer 192.168.1.26
```

clear ip msdp sa-cache

Use this command to clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries.

Command Syntax

```
clear ip msdp sa-cache (A.B.C.D |)
clear ip msdp (vrf NAME|) sa-cache (A.B.C.D |)
```

Parameters

A.B.C.D	Multicast group address; if not specified, all SA cache entries are cleared
NAME	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#clear ip msdp sa-cache 225.25.25.1
```

clear ip pim sparse-mode

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax

```
clear ip pim sparse-mode bsr rp-set *
clear ip pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rp-set`	PIMv2 bootstrap router RP set
`bsr`	PIMv2 Bootstrap Router
`*`	Clear all RP sets

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip pim sparse-mode bsr rp-set *
```

debug ip pim

Use this command to enable debugging for PIM.

Use the no option with this command to deactivate debugging for PIM.

Command Syntax

```
debug ip pim (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
debug ip pim (vrf
  NAME|)(all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
no debug ip pim (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
no debug ip pim (vrf NAME|) (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet
  |state|timer)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`all`	Enable debugging for all PIM events
`events`	Enable debugging for general configuration, VRF context
`mfc`	Enable debugging for MFC updates
`mib`	Enable debugging for MIB entries
`mtrace`	Enable debugging for MTRACE messages
`msdp`	Enable debugging for MSDP
`nexthop`	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
`nsm`	Enable debugging for NSM
`packet`	Enable debugging for PIM packets
`state`	Enable debugging for PIM states
`timer`	Enable debugging for PIM timers

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ip pim all
```

debug ip pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the no option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax

```
debug ip pim packet
debug ip pim packet in
debug ip pim packet out
debug ip pim (vrf NAME|) packet
debug ip pim (vrf NAME|) packet in
debug ip pim (vrf NAME|) packet out
no debug ip pim packet
no debug ip pim packet in
no debug ip pim packet out
no debug ip pim (vrf NAME|) packet
no debug ip pim (vrf NAME|) packet in
no debug ip pim (vrf NAME|) packet out
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
in	Debug incoming packets
out	Debug outgoing packets

Default

By default, all debug options are disabled.

Command Mode

Configure and Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip pim packet in
```

debug pim all

Use this command to enable debugging of all PIM events.

Use the no option with this command to disable debugging for PIM.

Command Syntax

```
debug pim all
debug pim (vrf NAME|) all
no debug pim all
no debug pim (vrf NAME|) all
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug pim all
```

debug ip pim timer assert

Use this command to enable debugging of the PIM assert timers.

Use the no option with this command to disable debugging for PIM assert timers.

Command Syntax

```
debug ip pim timer assert
debug ip pim timer assert at
debug ip pim (vrf NAME|) timer assert
debug ip pim (vrf NAME|) timer assert at
no debug ip pim timer assert
no debug ip pim timer assert at
no debug ip pim (vrf NAME|) timer assert
no debug ip pim (vrf NAME|) timer assert at
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
at	Use this option to turn on or off debugging of the PIM Assert Timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer assert at
```

debug ip pim timer bsr

Use this command to enable debugging of PIM BSR time.

Use the no option with this command to disable debugging of the PIM BSR timer.

Command Syntax

```
debug ip pim timer bsr
debug ip pim timer bsr bst
debug ip pim timer bsr crp
debug ip pim (vrf NAME|) timer bsr
debug ip pim (vrf NAME|) timer bsr bst
debug ip pim (vrf NAME|) timer bsr crp
no debug ip pim timer bsr
no debug ip pim timer bsr bst
no debug ip pim timer bsr crp
no debug ip pim (vrf NAME|) timer bsr
no debug ip pim (vrf NAME|) timer bsr bst
no debug ip pim (vrf NAME|) timer bsr crp
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`bst`	Turn on or turn off the bootstrap debugging timer
`crp`	Turn on or turn off the Candidate-RP debugging timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip pim timer bsr bst
```

debug ip pim timer hello

Use this command to enable debugging of various PIM Hello timers.

Use the no option with this command to disable debugging of the PIM Hello timers.

Command Syntax

```
debug ip pim timer hello
debug ip pim timer hello ht
debug ip pim timer hello nlt
debug ip pim timer hello tht
debug ip pim (vrf NAME|) timer hello
debug ip pim (vrf NAME|) timer hello ht
debug ip pim (vrf NAME|) timer hello nlt
debug ip pim (vrf NAME|) timer hello tht
no debug ip pim timer hello
no debug ip pim timer hello ht
no debug ip pim timer hello nlt
no debug ip pim timer hello tht
no debug ip pim (vrf NAME|) timer hello
no debug ip pim (vrf NAME|) timer hello ht
no debug ip pim (vrf NAME|) timer hello nlt
no debug ip pim (vrf NAME|) timer hello tht
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
ht	Turn on or turn off the PIM Hello debugging timer (ht)
nlt	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
tht	Turn on or turn off the Triggered Hello Timer (tht)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
```

```
(config)#debug ip pim timer hello ht
```

debug ip pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax

```
debug ip pim timer joinprune
debug ip pim timer joinprune et
debug ip pim timer joinprune kat
debug ip pim timer joinprune jt
debug ip pim timer joinprune ot
debug ip pim timer joinprune ppt
debug ip pim (vrf NAME|) timer joinprune
debug ip pim (vrf NAME|) timer joinprune et
debug ip pim (vrf NAME|) timer joinprune kat
debug ip pim (vrf NAME|) timer joinprune jt
debug ip pim (vrf NAME|) timer joinprune ot
debug ip pim (vrf NAME|) timer joinprune ppt
no debug ip pim timer joinprune
no debug ip pim timer joinprune et
no debug ip pim timer joinprune kat
no debug ip pim timer joinprune jt
no debug ip pim timer joinprune ot
no debug ip pim timer joinprune ppt
no debug ip pim (vrf NAME|) timer joinprune
no debug ip pim (vrf NAME|) timer joinprune et
no debug ip pim (vrf NAME|) timer joinprune kat
no debug ip pim (vrf NAME|) timer joinprune jt
no debug ip pim (vrf NAME|) timer joinprune ot
no debug ip pim (vrf NAME|) timer joinprune ppt
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`et`	Turn on or turn off the PIM JoinPrune expiry timer (et)
`jt`	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
`kat`	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)
`ot`	Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot)
`ppt`	Turn on or turn off the PIM JoinPrune PrunePending Timer ((ppt)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer joinprune et
```

debug ip pim timer register

Use this command to enable the PIM register timer's debugging.

Use the no option with this command to disable the PIM register timer's debugging.

Command Syntax

```
debug ip pim timer register
debug ip pim timer register rst
debug ip pim (vrf NAME|) timer register
debug ip pim (vrf NAME|) timer register rst
no debug ip pim timer register
no debug ip pim timer register rst
no debug ip pim (vrf NAME|) timer register
no debug ip pim (vrf NAME|) timer register rst
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rst`	Turn on or turn off the PIM Register Stop Timer (rst)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer register
```

ip msdp default-peer

Use this command to set a Multicast Source Discovery Protocol (MSDP) peer from which to accept Source-Active (SA) messages.

You can have multiple active default peers:

- When you enter multiple `ip msdp default-peer` commands *with* a `prefix-list` keyword, all the default peers are used at the same time for different RP prefixes. This form is typically used in a service provider cloud that connects stub site clouds.
- When you enter multiple `ip msdp default-peer` commands *without* a `prefix-list` keyword, a single active peer accepts all SA messages. If that peer fails, the next configured default peer accepts all SA messages. This form is typically used at a stub site.

Use the `no` option with this command to stop accepting SA messages from a peer.

Command Syntax

```
ip msdp default-peer A.B.C.D (prefix-list WORD|)
ip msdp (vrf NAME|) default-peer A.B.C.D (prefix-list WORD|)
no ip msdp default-peer A.B.C.D
no ip msdp (vrf NAME|) default-peer A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address of a previously configured MSDP peer
`prefix-list`	Make this the default peer only for an access list of rendezvous points (RPs):
`WORD`	Access list name
`NAME`	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ip msdp default-peer 192.168.1.26 prefix-list xyz
```

ip msdp mesh-group

Use this command to add a Multicast Source Discovery Protocol (MSDP) peer to a mesh group.

You can set up multiple mesh groups on the same device and multiple peers per mesh group.

Use the no option with this command to remove a peer from a mesh group.

Command Syntax

```
ip msdp mesh-group WORD A.B.C.D
ip msdp (vrf NAME|) mesh-group WORD A.B.C.D
no ip msdp mesh-group WORD A.B.C.D
no ip msdp (vrf NAME|) mesh-group WORD A.B.C.D
```

Parameters

WORD	Name of the mesh group
A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ip msdp mesh-group mg-1 192.168.1.26
```

ip msdp originator-id

Use this command to allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of an interface as a rendezvous point (RP) address in the SA message.

By default, OcNOS uses the RP address of the device.

Use the no option with this command to use the RP address of the device in SA messages.

Command Syntax

```
ip msdp originator-id IFNAME
ip msdp (vrf NAME|) originator-id IFNAME
no ip msdp originator-id IFNAME
no ip msdp (vrf NAME|) originator-id IFNAME
```

Parameters

IFNAME	Use the IP address of this interface as an RP address in SA messages
NAME	Name of the VPN routing/forwarding instance

Default

The RP address is used as the originator ID.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ip msdp originator-id eth2
```

ip msdp password

Use this command to set an MD5-shared password key used for authenticating a Multicast Source Discovery Protocol (MSDP) peer. By default, no MD5 password is enabled.

Use the no option with this command to remove a password.

Command Syntax

```
ip msdp password WORD peer A.B.C.D
ip msdp (vrf NAME|) password WORD peer A.B.C.D
no ip msdp password WORD peer A.B.C.D
no ip msdp (vrf NAME|) password WORD peer A.B.C.D
```

Parameters

WORD	Password
A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Default

The MD5 password authentication for TCP connections between MSDP peer is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ip msdp password S#m*u104!! peer 192.168.1.26
```

ip msdp peer

Use this command to configure an Multicast Source Discovery Protocol (MSDP) peer relationship.

Use the no option with this command to remove a peer relationship.

Command Syntax

```
ip msdp peer A.B.C.D ((connect-source (IFNAME))|)
ip msdp (vrf NAME|) peer A.B.C.D ((connect-source (IFNAME))|)
ip msdp peer A.B.C.D connect-source A.B.C.D
ip msdp (vrf Name|) peer A.B.C.D connect-source A.B.C.D
no ip msdp peer A.B.C.D
no ip msdp (vrf NAME|) peer A.B.C.D
```

Parameters

A.B.C.D	IP address of the potential peer
A.B.C.D	IP address of local peer
IFNAME	Use the primary address of this interface for the TCP connection with the peer
NAME	Name of the VPN routing/forwarding instance

Default

By default, all ip msdp options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ip msdp peer 192.168.1.26 connect-source eth2
```

ip pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

Use the no option with this command to revert to default.

Command Syntax

```
ip pim accept-register list WORD
ip pim (vrf NAME|) accept-register list WORD
no ip pim accept-register
no ip pim (vrf NAME|) accept-register
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
WORD	Name of a standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim accept-register list xyz

(config)#no ip pim accept-register
```

ip pim anycast-rp

Use this command to configure the Anycast RP in the RP set.

Use the no option with this command to remove the configuration.

Command Syntax

```
ip pim anycast-rp A.B.C.D A.B.C.D
ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
no ip pim anycast-rp A.B.C.D
no ip pim anycast-rp A.B.C.D A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`A.B.C.D`	Unicast IP address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
`A.B.C.D`	Destination IP address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ip pim anycast-rp 1.1.1.1 10.10.10.10
```

ip pim bidir-enable

Use this command to enable Bidirectional PIM.

Use the no option with this command to disable Bidirectional PIM.

Command Syntax

```
ip pim bidir-enable
no ip pim bidir-enable
```

Parameters

None

Default

By default, bidirectional pim is disabled.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-enable

#configure terminal
(config)#no ip pim bidir-enable
```

ip pim bidir-offer-interval

Use this command to configure the bidirectional pim designated forwarder (DF) election offer message interval time. Time interval default unit is seconds.

Use the no command to revert the offer interval period configuration to the default value.

Command Syntax

```
ip pim bidir-offer-interval <1-20000> (msec|)
no ip pim bidir-offer-interval
```

Parameters

msec	Specify interval time in milliseconds

Default

The default value for interval time is 100 ms.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-offer-interval 123 msec
(config)#no ip pim bidir-offer-interval
```

ip pim bidir-offer-limit

Use this command to configure the number of unanswered offers before the device changes the interface state to the designated forwarder (DF) Winner

Use the no command to reset the offer limit to its default

Command Syntax

```
ip pim bidir-offer-limit <4-100>
no ip pim bidir-offer-limit
```

Parameters

<4-100>	Specify the limit of unanswered offers.

Default

The default value is three unanswered offers.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-offer-limit 50
(config)#no ip pim bidir-offer-limit
```

ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

When this command is configured on an interface, no PIM Version 2 BSR messages are sent or received through the interface. Use this command to configure an interface bordering another PIM domain to avoid the exchange of BSR messages between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in a protocol malfunction or loss of isolation between the domains.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Use the no option with this command to remove the BSR border configuration.

Command Syntax

```
ip pim bsr-border
no ip pim bsr-border
```

Default

By default, the ip pim bsr-border is disabled.

Parameters

None

Default

Bootstrap router border configuration is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures the interface to be the PIM domain border:

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim bsr-border

(config)#interface eth0
(config-if)#no ip pim bsr-border
```

ip pim bsr-candidate

Use this command to give the router the candidate BSR status using the specified IP address of the interface.

Use the no option with this command to disable this function.

Command Syntax

```
ip pim bsr-candidate IFNAME
ip pim bsr-candidate IFNAME <0-32>
ip pim bsr-candidate IFNAME <0-32> <0-255>
ip pim (vrf NAME|) bsr-candidate IFNAME
ip pim (vrf NAME|) bsr-candidate IFNAME <0-32>
ip pim (vrf NAME|) bsr-candidate IFNAME <0-32> <0-255>
no ip pim bsr-candidate (IFNAME|)
no ip pim (vrf NAME|) bsr-candidate (IFNAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
IFNAME	Specify the name of the interface
<0-32>	Specify a hash mask length for RP selection
<0-255>	Specify a priority for a BSR candidate

Default

The router is not configured to announce itself as a candidate BSR.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim bsr-candidate eth0 20 30
```

ip pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to revert to the default settings.

Command Syntax

```
ip pim cisco-register-checksum
ip pim cisco-register-checksum group-list WORD
ip pim (vrf NAME|) cisco-register-checksum
ip pim (vrf NAME|) cisco-register-checksum group-list WORD
no ip pim cisco-register-checksum
no ip pim cisco-register-checksum group-list WORD
no ip pim (vrf NAME|) cisco-register-checksum
no ip pim (vrf NAME|) cisco-register-checksum group-list WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`group-list`	Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.
`WORD`	IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim cisco-register-checksum

#configure terminal
(config)#ip pim cisco-register-checksum group-list xyz
(config)#ip access-list 34 permit 224.0.1.3
```

ip pim

Use this command to enable PIM dense-mode or sparse-mode on the current interface.

Use the `no` option with this command to disable PIM dense-mode or sparse-mode or sparse-dense-mode on the interface.

Command Syntax

```
ip pim (dense-mode|sparse-mode)
no ip pim (dense-mode|sparse-mode)
```

Parameters

`dense-mode`	Enable PIM dense-mode operation
`sparse-mode`	Enable PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode

(config)#interface eth0
(config-if)#no ip pim dense-mode

(config)#interface eth0
(config-if)#ip pim sparse-mode

(config-if)#no ip pim sparse-mode
```

ip pim passive

Use this command to enable or disable passive mode operation for local members on the interface. Passive mode essentially stops PIM transactions on the interface, allowing only the Internet Group Management Protocol (IGMP) mechanism to be active.

Use the no option with this command to disable the passive mode.

Command Syntax

```
ip pim (dense-mode|sparse-mode) passive
no ip pim (dense-mode|sparse-mode) passive
```

Parameters

`dense-mode`	Enable passive operation for PIM dense-mode
`sparse-mode`	Enable passive operation for PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode passive

(config)#interface eth0
(config-if)#no ip pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ip pim sparse-mode passive

(config)#interface eth0
(config-if)#no ip pim sparse-mode passive
```

ip pim dr-priority

Use this command to set the designated router's priority value.

Use the no option with this command to remove the priority from the DR.

Command Syntax

```
ip pim dr-priority <0-4294967294>
no ip pim dr-priority (<0-4294967294>|)
```

Parameter

`<0-4294967294>` Valid range of values for DR priority, with a higher value resulting in a higher preference

Default

The default DR priority value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dr-priority 11234

(config)#interface eth0
(config-if)#no ip pim dr-priority 11234
```

ip pim exclude-genid

Use this command to exclude the GenID (generated ID) option from Hello packets sent by the PIM module on an interface. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to restore PIM to its default setting.

Command Syntax

```
ip pim exclude-genid
no ip pim exclude-genid
```

Parameters

None

Default

By default, the ip pim exclude-genid command is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Default

By default, this command is disabled; that is, the GenID option is included.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim exclude-genid

(config)#interface eth0
(config-if)#no ip pim exclude-genid
```

ip pim hello-holdtime

Use this command to configure a hello holdtime other than the default(`3.5 * hello_interval` seconds).

When configuring `hello-holdtime`, if the configured value is less than the current `hello_interval`, it is refused.

When removing a configured `hello_holdtime`, the value is reset to (`3.5 *` current `hello_interval`) value.

Every time the hello_interval is updated, the hello-holdtime is also updated according to rules below:

If the hello_holdtime is not configured, or if the hello_holdtime is configured, but is less than the current hello_interval value, it is modified to (3.5 * hello_interval). Otherwise, the configured value is maintained.

Use the `no` option with this command to remove the configured hello-holdtime.

Command Syntax

```
ip pim hello-holdtime <1-65535>
no ip pim hello-holdtime
```

Parameter

`<1-65535>`	Range of values for hello-holdtime, in seconds

Default

The default hello-holdtime is 105 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-holdtime 123

(config)#interface eth0
(config-if)#no ip pim hello-holdtime
```

ip pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the no option with this command to reset the hello-interval to its default value.

Command Syntax

```
ip pim hello-interval <1-18724>
no ip pim hello-interval
```

Parameter

<1-18724>	Range of values for the hello-interval. No fractional values are allowed in seconds.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-interval 123

(config)#interface eth0
(config-if)#no ip pim hello-interval
```

ip pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to remove this setting.

Command Syntax

```
ip pim ignore-rp-set-priority
ip pim (vrf NAME|) ignore-rp-set-priority
no ip pim ignore-rp-set-priority
no ip pim (vrf NAME|) ignore-rp-set-priority
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim ignore-rp-set-priority

#configure terminal
(config)#no ip pim ignore-rp-set-priority
```

ip pim jp-timer

Use this command to set a PIM join/prune timer.

Use the no option with this command to remove the join/prune timer.

Command Syntax

```
ip pim jp-timer <1-65535>
ip pim (vrf NAME|) jp-timer <1-65535>
no ip pim jp-timer
no ip pim jp-timer <1-65535>
no ip pim (vrf NAME|) jp-timer
no ip pim (vrf NAME|) jp-timer <1-65535>
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for the Join/Prune timer, in seconds

Default

The ip pim jp-timer default value is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim jp-timer 234

#configure terminal
(config)#no ip pim jp-timer 234
```

ip pim neighbor-filter

Use this command to enable filtering of neighbors on the interface. When configuring a neighbor filter, PIM either not establish adjacency with neighbor or terminates adjacency with existing neighbors, when denied by filtering access list.

Use the no option with this command to disable filtering of neighbors on the interface.

Command Syntax

```
ip pim neighbor-filter WORD
no ip pim neighbor-filter WORD
```

Parameters

WORD	Name of an IP standard access list

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Default

This command is disabled by default there is no filtering.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim neighbor-filter xyz
(config-if)#exit
(config)#ip access-list deny 192.168.1.53
(config)#ip access-list permit any
```

ip pim propagation-delay

Use this command to configure a propagation delay value for PIM.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax

```
ip pim propagation-delay <0-32767>
no ip pim propagation-delay
```

Parameter

<0-32767>	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 500 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ip pim propagation-delay
```

ip pim register-rate-limit

Use this command to configure the rate of Register packets sent by this designated router (DR), in number of packets per second.

Use the no option to remove the register-rate-limit configuration.

Note: The configured rate is per (S,G) state, and is not a system-wide rate.

Command Syntax

```
ip pim register-rate-limit <1-65535>
ip pim (vrf NAME|) register-rate-limit <1-65535>
no ip pim register-rate-limit <1-65535|>
no ip pim (vrf NAME|) register-rate-limit <1-65535|>
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for packets to send per second

Default

No rate limit is set for PIM-SM register packets.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rate-limit 3444

#configure terminal
(config)#no ip pim register-rate-limit
```

ip pim register-rp-reachability

Use this command to enable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to disable the RP reachability check for PIM Registers at the DR.

Note: “ip pim register-rp-reachability” is default configuration and it would not be shown in running-configuration, even if admin configures it. If admin does "no" command of this configuration, it would be shown in running-configuration.

Command Syntax

```
ip pim register-rp-reachability
ip pim (vrf NAME|) register-rp-reachability
no ip pim register-rp-reachability
no ip pim (vrf NAME|) register-rp-reachability
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

The default setting is checking for rendezvous point reachability,

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rp-reachability
```

ip pim register-source

Use this command to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the no option to remove the source address of register packets sent by this DR, and reset it to use the default source address, that is, the address of the RPF interface toward the source host.

The configured address must be a reachable address so the RP can send corresponding Register-Stop messages in response. This address is usually the loopback interface address, but can also be other physical addresses. The address must be advertised by unicast routing protocols on the DR.

Note: The interface configured does not require PIM to be enabled.

Command Syntax

```
ip pim register-source A.B.C.D
ip pim register-source IFNAME
ip pim (vrf NAME|) register-source A.B.C.D
ip pim (vrf NAME|) register-source IFNAME
no ip pim register-source (A.B.C.D|)
no ip pim register-source (IFNAME|)
no ip pim (vrf NAME|) register-source (A.B.C.D|)
no ip pim (vrf NAME|) register-source (IFNAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	The IP address to use as the source of the register packets
IFNAME	The name of the interface to use as the source of the register packets

Default

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-source 3.3.3.2
```

ip pim register-suppression

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR; configuring this value at the RP modifies the RP-keepalive-period value if the `ip pim rp-register-kat` command is not used.

Use the no option to remove the register-suppression setting.

Command Syntax

```
ip pim register-suppression <1-65535>
ip pim (vrf NAME|) register-suppression <1-65535>
no ip pim register-suppression
no ip pim (vrf NAME|) register-suppression
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for register suppression time in seconds

Default

By default, the ip pim option is disabled.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim register-suppression 555

#configure terminal
(config)#no ip pim register-suppression
```

ip pim router-id

Use this command to configure PIM router-ID to uniquely identify the router.By default, PIM registers for the NSM router-id service. This command will override the router-id received from NSM.

Use the `no` option with this command to unconfigure PIM router-ID. This will make PIM fall back to the NSM router-id

Command Syntax

```
ip pim (vrf NAME|) router-id A.B.C.D
no ip pim (vrf NAME|) router-id A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	Specify the Router ID

Default

By default, the ip pim option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim router-id 1.1.1.1

(config)#no ip pim router-id 1.1.1.1
```

ip pim rp-address

Use this command to statically configure Rendezvous Point (RP) address for multicast groups.

Use the no option to remove the RP address.

OcNOS PIM supports multiple static RPs. It also supports static-RP and Bootsrtrap Router (BSR) mechanism simultaneously. The following list states the correct usage of this command:

- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen over statically configured RP-address.
- One static-RP can be configured for multiple group ranges using Access Lists. However, configuring multiple static RPs (using `ip pim rp-address` command) with the same RP address is not allowed. The static-RP can either be configured for the whole multicast group range `224/4` (without ACL) or for specific group ranges (using ACL). For example, configuring `ip pim rp-address 1.2.3.4` will configure static-RP 1.2.3.4 for the default group range `224/4`. Configuring `ip pim rp-address 5.6.7.8 grp-list` will configure static-RP `5.6.7.8` for all the group ranges represented by `Permit` filters in `grp-list` ACL.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
- Only `permit` filters in ACL are considered as valid group ranges. The default `Permit` filter `0.0.0.0/0` is converted to default multicast filter `224/4`.
- When selecting static-RPs for a group range, the first element, with the static-RP with highest IP address, is chosen.
- Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ip pim rp-address` command without the `override` keyword. Commands with the `override` keyword take precedence over dynamically learned mappings.

Command Syntax

```
ip pim rp-address A.B.C.D (override|)
ip pim rp-address A.B.C.D WORD (override|)
ip pim rp-address A.B.C.D WORD (bidir|)
ip pim (vrf NAME|) rp-address A.B.C.D (override|)
ip pim (vrf NAME|) rp-address A.B.C.D WORD (override|)
ip pim (vrf NAME|) rp-address A.B.C.D WORD (bidir|)
no ip pim rp-address A.B.C.D
no ip pim rp-address A.B.C.D WORD
no ip pim (vrf NAME|) rp-address A.B.C.D
no ip pim (vrf NAME|) rp-address A.B.C.D WORD
```

Parameters

`Bidir`	Bidirectional RP address
`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Standard Access-list name
`override`	Static RP overrides dynamically-learned RP

Default

No PIM static group-to-RP mappings are configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#ip pim rp-address 3.3.3.3 xyz
(config)#ip pim rp-address 2.2.2.2 ip1 bidir
```

ip pim rp-candidate

Use this command to give the router a candidate RP status using the IP address of the specified interface.

Use the no option along with this command to remove the settings.

Command Syntax

```
ip pim rp-candidate IFNAME (bidir|) ((group-list WORD)|) (interval <0-16383>|)
  (priority <0-255>|)
ip pim (vrf NAME) rp-candidate IFNAME (bidir|) ((group-list WORD)|) (interval <0-
  16383>|) (priority <0-255>|)
no ip pim rp-candidate (IFNAME|)
no ip pim (vrf NAME) rp-candidate (IFNAME|)
```

Parameters

`vrf NAME`	The VPN routing/forwarding instance
`IFNAME`	Specify an interface name
`WORD`	A named standard access list
`group-list`	Group Ranges for this C-RP
`interval`	C-RP advertisement interval
`priority`	Candidate-RP priority
`<0-16383>`	Range of values for candidate-RP advertisement interval, in seconds
`<0-255>`	Range of values for priority of an RP candidate

Default

The ip pim rp-candidate default priority is 192 and interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim rp-candidate eth0

(config)#no ip pim rp-candidate eth0
```

ip pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value.

Use the no option to remove this configuration.

Command Syntax

```
ip pim rp-register-kat <1-65535>
ip pim (vrf NAME|) rp-register-kat <1-65535>
no ip pim rp-register-kat
no ip pim (vrf NAME|) rp-register-kat
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for a KAT time in seconds

Default

The ip pim rp-register-kat default is 60 seconds.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim rp-register-kat 3454

(config)#no ip pim rp-register-kat
```

ip pim spt-threshold

Use this command to turn on the ability of the last-hop PIM router to switch to SPT.

Use the no option with this command to turn off the ability of the last-hop PIM router to switch to SPT.

Note: This option is binary, meaning that the switching to SPT happens either at the receiving of the first data packet or not at all. It is not rate-based.

Command Syntax

```
ip pim spt-threshold
ip pim spt-threshold group-list WORD
ip pim (vrf NAME|) spt-threshold
ip pim (vrf NAME|) spt-threshold group-list WORD
no ip pim spt-threshold
no ip pim spt-threshold group-list WORD
no ip pim (vrf NAME|) spt-threshold
no ip pim (vrf NAME|) spt-threshold group-list WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`group-list`	Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list
`WORD`	A named standard access list

Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim spt-threshold

#configure terminal
(config)#ip pim spt-threshold group-list LIST1
(config)#ip access-list permit 224.0.1.3

#configure terminal
(config)#no ip pim spt-threshold
```

ip pim ssm

Use this command to configure Source Specific Multicast (SSM) and define the range of multicast IP addresses. The keyword `default` defines the SSM range as 232/8. To define an SSM range other than the default, specify an access-list.

When an SSM range of IP multicast addresses is defined with this command, the no (*,G) or (S,G,rpt) state is initiated for groups in the SSM range.

The messages corresponding to these states are not accepted and originate in the SSM range.

Use the `no` form of this command to disable the SSM range.

Command Syntax

```
ip pim ssm default
ip pim ssm range WORD
ip pim (vrf NAME|) ssm default
ip pim (vrf NAME|) ssm range WORD
no ip pim ssm
no ip pim (vrf NAME|) ssm
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`default`	This keyword defines the 232/8 group range for SSM
`range`	Define an access-list for group range to use for SSM
`WORD`	A named standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ip pim ssm range xyz
```

ip pim state-refresh origination-interval

Use this command to configure a PIM-DM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM-DM State Refresh control messages.

Use the no option with this command to return the origination interval to its default value.

Command Syntax

```
ip pim state-refresh origination-interval <1-100>
no ip pim state-refresh origination-interval
```

Parameter

<1-100>	Range of values for state-refresh origination interval, in seconds

Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ip pim state-refresh origination-interval
```

ip pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the no option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax

```
ip pim unicast-bsm
no ip pim unicast-bsm
```

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim unicast-bsm

(config)#interface eth0
(config-if)#no ip pim unicast-bsm
```

show debugging ip pim

Use this command to display the debug status for the PIM process.

Command Syntax

```
show debugging ip pim
show debugging ip pim (vrf NAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ip pim
 PIM Debugging status:
 PIM event debugging is on
 PIM MFC debugging is on
 PIM state debugging is on
 PIM incoming packet debugging is on
 PIM outgoing packet debugging is on
 PIM Hello HT timer debugging is on
 PIM Hello NLT timer debugging is on
 PIM Hello THT timer debugging is on
 PIM Join/Prune JT timer debugging is on
 PIM Join/Prune ET timer debugging is on
 PIM Join/Prune PPT timer debugging is on
 PIM Join/Prune KAT timer debugging is on
 PIM Join/Prune OT timer debugging is on
 PIM Assert AT timer debugging is on
 PIM Register RST timer debugging is on
 PIM Bootstrap BST timer debugging is on
 PIM Bootstrap CRP timer debugging is on
 PIM mib debugging is on
 PIM nexthop debugging is on
 PIM mtrace debugging is on
 PIM NSM debugging is on
 PIM MSDP debugging is on
```

show debugging pim

Use this command to display the status of debugging for PIM.

Command Syntax

```
show debugging pim
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This command displays one of several status:

```
#show debugging pim
PIM Debugging status:
  PIM event debugging is on
  PIM MFC debugging is on
  PIM state debugging is on
  PIM incoming packet debugging is on
  PIM outgoing packet debugging is on
  PIM Hello HT timer debugging is on
  PIM Hello NLT timer debugging is on
  PIM Hello THT timer debugging is on
  PIM Join/Prune JT timer debugging is on
  PIM Join/Prune ET timer debugging is on
  PIM Join/Prune PPT timer debugging is on
  PIM Join/Prune KAT timer debugging is on
  PIM Join/Prune OT timer debugging is on
  PIM Assert AT timer debugging is on
  PIM Register RST timer debugging is on
  PIM Bootstrap BST timer debugging is on
  PIM Bootstrap CRP timer debugging is on
  PIM mib debugging is on
  PIM nexthop debugging is on
  PIM mtrace debugging is on
  PIM NSM debugging is on
  PIM MSDP debugging is on
```

show ip msdp peer

Use this command to display information about a Multicast Source Discovery Protocol (MSDP) peer.

Command Syntax

```
show ip msdp peer (A.B.C.D|)
show ip msdp (vrf NAME|) peer (A.B.C.D|)
```

Parameters

A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ip msdp peer

MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

Table 1-35: show ip msdp peer output

Entry	Description
MSDP Peer	IP address of the peer
Connection status	State – Up, Down, Invalid, Disabled, Inactive, Listening, Connecting, Established, or Maximum. Keepalive sent – Keepalive messages sent to peer. Keepalive received – Keepalive messages received from the peer. number of connect retries – Number of peer connect retries.

show ip msdp sa-cache

Use this command to display the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

You can specify zero, one, or two addresses:

- If you do not specify any address, the entire Source-Active (SA) cache is displayed.
- If you specify only a unicast address it is treated as a source; if you specify only a multicast address it is treated as a group. In either case, entries corresponding to that address are displayed.
- If you specify two addresses, an (S, G) entry corresponding to those addresses is displayed; one address must be unicast and the other address must be multicast.

Command Syntax

```
show ip msdp sa-cache
show ip msdp sa-cache details
show ip msdp sa-cache A.B.C.D
show ip msdp sa-cache A.B.C.D A.B.C.D
show ip msdp (vrf NAME|) sa-cache
show ip msdp (vrf NAME|) sa-cache details
show ip msdp (vrf NAME|) sa-cache A.B.C.D
show ip msdp (vrf NAME|) sa-cache A.B.C.D A.B.C.D
```

Parameters

`A.B.C.D`	Source and/or group IP address
`details`	Detailed sa-cache information
`NAME`	Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02
Exptime  00:03:28P
```

Table 1-36: show ip msdp sa-cache output

Entry	Description
MSDP Source-Active Cache	• (S,G) address pair – Source address, multicast address • RP – Reverse Path address • RRF-Peer – Reverse Path Forwarding address • Uptime – as stated • Exptime – Time until entry timeout

show ip pim interface

Use this command to display PIM interface information.

Command Syntax

```
show ip pim interface
show ip pim interface detail
show ip pim (vrf NAME|) interface
show ip pim (vrf NAME|) interface detail
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
detail	Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
Router_E#show ip pim interface
Address         Interface  VIFindex Ver/   Nbr      DR      DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

The output for PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  interface detail
eth1 (vif 0):
  Address 192.168.10.57, DR 192.168.10.57
  Hello period 30 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 3
  Neighbors:
   192.168.10.52

eth2 (vif 2):
  Address 192.168.1.57, DR 192.168.1.152
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 4
  ECMP REDIRECT, bundle : ecmpbundle, status :  allowed
  Neighbors:
```

```
192.168.1.149
192.168.1.150
192.168.1.152
```

Table 1-37: Show ip pim interface output

Entry	Description
Address	IP address of the interface
Interface	Interface name (eth1, xe3, ge4/1, etc.).
VIFindex	The index number of the Virtual Host Interface (vif).
Ver/Mode	PIM version (either v1, v2, or v3) / PIM Mode – Either S (sparse mode) or D (dense mode).
Nbr Count	Neighbor Count.
DR Prior	Designated Router Priority.
DR	Address of the Designated Router.
Hello Period	Routing devices send hello messages at a fixed interval on all PIM-enabled interfaces. By using hello messages, routing devices advertise their existence as PIM routing devices on the subnet.
Next Hello	When the interval counts down to 0, the routing device sends another hello message, and the timer is reset. A routing device that receives no response from a neighbor in 3.5 times the interval value drops the neighbor.
Propagation Delay	Vif Hello LAN Delay – propagation delay in milliseconds.
ECMP Redirect, bundle	An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.
Neighbors	A list of the addresses of PIM multicast neighbors.

show ip pim interface df

Use this command to display Bidirectional-PIM Designated Forwarder(DF) election status.

Command Syntax

```
show ip pim interface (IFNAME|) df (A.B.C.D|)
```

Parameters

IFNAME	Name of the interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
Router# show ip pim interface df

Interface RP          DF Winner   Metric
eth1      10.10.0.2   10.4.0.2    0
          10.10.0.3   10.4.0.3    0
          10.10.0.5   10.4.0.4    409600
eth2      10.10.0.2   10.5.0.2    0

Router# show ip pim interface eth1 df 10.10.0.3

Designated Forwarder election for eth1, 10.4.0.2, RP 10.10.0.3
   State Non-DF
   Offer count is 0
   Current DF ip address 10.4.0.3
   Last winner metric preference 0
   Last winner metric 0
```

show ip pim mroute

Use this command to display information in the IP PIM multicast routing table.

Command Syntax

```
show ip pim mroute (detail|)
show ip pim mroute A.B.C.D (detail|)
show ip pim mroute A.B.C.D A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D A.B.C.D (detail|)
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	Display all entries for this group IP address
`A.B.C.D`	Display all entries for this source IP address

Note: A group IP address and a source IP address cannot be simultaneously

`detail`	Display detailed PIM multicast routing table information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim mroute

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
 Outgoing  o..............................
```

Table 1-38: Show ip pim mroute output

Entry	Description
(*, *, RP) Entries:	Source, Group, Rendezvous Point Include entries.
(*, G) Entries:	PIM Include entries
(S, G) Entries:	PIM Include entries (Source, Group)
(S, G, rpt) Entries:	The RPT is the path between the RP and receivers (hosts) in a multicast group. The RPT is built by means of a PIM join message from a receiver's DR.
RP:	Rendezvous Point
RPF nbr:	Reverse Path Forwarding neighbor.
RPF idx:	Reverse Path Forwarding index.
Upstream State:	As stated.

show ip pim neighbor

Use this command to display PIM neighbor information.

Command Syntax

```
show ip pim neighbor (detail|)
show ip pim neighbor IFNAME (detail|)
show ip pim neighbor IFNAME A.B.C.D (detail|)
show ip pim (vrf NAME|) neighbor (detail|)
show ip pim (vrf NAME|) neighbor IFNAME (detail|)
show ip pim (vrf NAME|) neighbor IFNAME A.B.C.D (default|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
IFNAME	Name of the interface
A.B.C.D	IPv4 address of the neighbor interface
detail	Display detailed information for a PIM neighbor

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip pim neighbor
Neighbor      Interface    Uptime/Expires     Ver          DR
Address                                                Priority/Mode
10.10.14.11    eth3       00:14:30/00:01:45    v2         1 / DR
```

The validation command to view PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  neighbor detail
Nbr 192.168.10.52 (eth1)
Expires in 83 seconds, uptime 00:21:52
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 1048865461,

Nbr 192.168.1.149 (eth2)
Expires in 99 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 2102076842,
Interface ID: Router-ID: 1.1.1.149 Local-ID: 4,
ECMP REDIRECT enabled
```

```
Nbr 192.168.1.150 (eth2)
Expires in 77 seconds, uptime 00:22:02
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 1306457151,
Interface ID: Router-ID: 1.1.1.153 Local-ID: 4,
ECMP REDIRECT enabled

Nbr 192.168.1.152 (eth2), DR
Expires in 86 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 170629600,
Interface ID: Router-ID: 1.1.1.152 Local-ID: 4,
ECMP REDIRECT enabled
```

Table 1-39: Show ip pim neighbor output

Entry	Description
Neighbor	Neighbor IP address
Interface	Name of the interface (eth1, xe3, xe5/1 etc.).
Uptime/Expires	Neighbor’s uptime / time until uptime expires and starts sending hello messages.
Ver	PIM version (version1 =v1, version2 - v2, version3 = v3).
DR Priority/mode	Priority and Mode of neighbor as Designated Router.
Nbr	NEighbor IP address and interface name (eth1, xe3, xe5/1 etc.).
Expires in	Time before the Hello timer expires and must retransmit.
uptime	Neighbor uptime.
Holdtime:	Before an interface goes down or changes primary IP address, a Hello message with a zero HoldTime should be sent immediately (with the old IP address if the IP address changed). This will cause PIM neighbors to remove this neighbor (or its old IP address) immediately. After an interface has changed its IP address, it MUST send a Hello message with its new IP address. If an interface changes one of its secondary IP addresses, a Hello message with an updated Address_List option and a non-zero HoldTime should be sent immediately. This will cause PIM neighbors to update this neighbor's list of secondary addresses immediately.
T-bit:	RPT-bit is a 1-bit value. The RPT-bit is set to 1 for Assert(*,G) messages and 0 for Assert(S,G) messages.

Table 1-39: Show ip pim neighbor output

Entry	Description
Lan delay:	In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: neighbor.lan_prune_delay_present A flag indicating if the LAN Prune Delay option was present in the Hello message. neighbor.tracking_support A flag storing the value of the T bit in the LAN Prune Delay option if it is present in the Hello message. This indicates the neighbor's capability to disable Join message suppression. neighbor.propagation_delay The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message. neighbor.override_interval The Override_Interval field of the LAN Prune Delay option (if present) in the Hello message. The additional state described above is deleted along with the DR neighbor state when the neighbor timeout expires.
Override interval:	Hello Override Interval
DR priority:	The DR_Priority Option allows a network administrator to give preference to a particular router in the DR election process by giving it a numerically larger DR Priority.The DR_Priority Option SHOULD be included in every Hello message, even if no DR Priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR_Priority Option. The default priority is 1.
Gen ID:	Generation Identifier, used to detect reboots.
Interface ID:	As stated.
Router-ID:	As stated.
Local-ID:	As stated.
ECMP REDIRECT	Whether ECMP Redirect is enabled or disabled.

show ip pim nexthop

Displays the nexthop information from NSM as used by PIM.

Command Syntax

```
show ip pim nexthop
show ip pim (vrf NAME|) nexthop
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim nexthop
```

show ip pim bsr-router

Use this command to show the bootstrap router PIMv2 address.

Command Syntax

```
show ip pim bsr-router
show ip pim (vrf NAME|) bsr-router
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 10.10.11.35 (?)
  Uptime:      00:00:38, BSR Priority: 0, Hash mask length: 10
  Expires:     00:01:32
  Role: Non-candidate BSR
  State: Accept Preferred

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

Table 1-40: Show ip pim bsr-router output

Entry	Description
BSR address	Bootstrap Router’s IP address.
Uptime	As stated
BSR Priority	BSR election priority; can be set manually, but default is 64.
Hash mask length	As stated.
Expires	Group-to-C-RP mapping Expiry Timer.

Table 1-40: Show ip pim bsr-router output (Continued)

Entry	Description
Role	Specifies whether the BSR is the Candidate BSR or a Non-candidate BSR
State	• The current state of a Candidate BSR, one of the following: Candidate-BSR, Pending-BSR, or Elected-BSR. • The current state of a Non-candidate BSR, one of the following: Accept Any or Accept Preferred.

show ip pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax

```
show ip pim local-members
show ip pim local-members IFNAME
show ip pim (vrf NAME|) local-members
show ip pim (vrf NAME|) local-members IFNAME
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
IFNAME	Display local membership for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim vrf q local-members p8p1
PIM Local membership information

p8p1:
  (*, 233.5.5.5) : Include
  (*, 233.7.7.7) : Include
```

Table 1-41: Show ip pim local-members output

Entry	Description
NAME:	Interface name
(*,G)	The local members in the form (Source/Group). Shows state – either Include or Exclude.

show ip pim rp-hash

Use this command to display the rendezvous point (RP) to chose based on the group selected.

Command Syntax

```
show ip pim rp-hash A.B.C.D
show ip pim (vrf NAME|) rp-hash A.B.C.D
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

A.B.C.D in command refers to the group address to be hashed.

```
#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

Table 1-42: Show ip PIM rp-hash output

Entry	Description
Group(s)	The group address to be hashed.
RP	Rendezvous Point
Info source	The address and identity from which this information was received. In the example above, it was learned from the bootstrap router.

show ip pim rp mapping

Use this command to show group-to-RP (rendezvous point) mappings, and the RP set.

Command Syntax

```
show ip pim rp mapping
show ip pim (vrf NAME|) rp mapping
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim rp mapping
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 10.10.1.5
    Info source: 172.16.1.2, via bootstrap, priority 192
         Uptime: 00:00:13, expires: 00:02:29
 RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:34:42, expires: 00:01:49
```

Table 1-43: Show ip PIM rp mapping output

Entry	Description
Identity declaration	This system is the Bootstrap Router (PIM version number v1, v2. or, v3) or not the Bootstrap Router.
Group(s):	The Multicast address of this multicast Group.
RP	Addresses of the Rendezvous Points.
Info source:	Address of the info source, whether it was learned from the Bootstrap Router, and the configured priority.

snmp restart pim

Use this command to restart SNMP in (PIM).

Note: This command restarts IPv4 PIM daemon

Command Syntax

```
snmp restart pim
```

Parameters

None

Default

By default, the snmp restart pim is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart pim
```

undebug all ip pim

Use this command to disable all PIM debugging from Configure mode.

Command Syntax

```
undebug all ip pim
undebug (vrf NAME|) all ip pim
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#undebug all ip pim
```

CHAPTER 2 PIMv6 Commands

This chapter describes the commands for Protocol-Independent Multicast (PIM).

- ipv6 pim rp-candidate
- ipv6 pim rp-register-kat
- ipv6 pim spt-threshold
- ipv6 pim ssm
- ipv6 pim state-refresh origination-interval
- ipv6 pim unicast-bsm
- show debugging ipv6 pim
- show ipv6 pim interface
- show ipv6 pim mroute
- show ipv6 pim neighbor
- show ipv6 pim nexthop
- show ipv6 pim bsr-router
- show ipv6 pim local-members
- show ipv6 pim rp-hash
- show ipv6 pim rp mapping
- undebug all ipv6 pim

clear ipv6 mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax

```
clear ipv6 mroute *
clear ipv6 mroute * pim (dense-mode|sparse-mode)
clear ipv6 mroute X:X::X:X
clear ipv6 mroute X:X::X:X X:X::X:X
clear ipv6 mroute X:X::X:X X:X::X:X pim (dense-mode|sparse-mode)
clear ipv6 mroute X:X::X:X pim sparse-mode
clear ipv6 mroute statistics *
clear ipv6 mroute statistics X:X::X:X
clear ipv6 mroute statistics X:X::X:X X:X::X:X
clear ipv6 mroute (vrf NAME|) *
clear ipv6 mroute (vrf NAME|) * pim (dense-mode|sparse-mode)
clear ipv6 mroute (vrf NAME|) X:X::X:X
clear ipv6 mroute (vrf NAME|) X:X::X:X X:X::X:X
clear ipv6 mroute (vrf NAME|) X:X::X:X X:X::X:X pim (dense-mode|sparse-mode)
clear ipv6 mroute (vrf NAME|) X:X::X:X pim sparse-mode
clear ipv6 mroute (vrf NAME|) statistics *
clear ipv6 mroute (vrf NAME|) statistics X:X::X:X
clear ipv6 mroute (vrf NAME|) statistics X:X::X:X X:X::X:X
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`*`	Delete all multicast routes
`statistics`	Clears multicast route statistics
`X:X::X:X`	Clears group IP address
`X:X::X:X`	Clears source IP address
`dense-mode`	Clear multicast rout table for PIM dense-mode
`sparse-mode`	Clear multicast route table for PIM sparse mode

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 mroute * pim sparse-mode
#clear ipv6 mroute 3ffe::24:3 ff00::3 pim sparse-mode
```

clear ipv6 pim sparse-mode bsr

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax

```
clear ipv6 pim sparse-mode bsr rp-set *
clear ipv6 pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`rp-set`	PIMv2 bootstrap router RP set
`*`	Clear all RP sets
`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 pim sparse-mode bsr rp-set *
```

debug ipv6 pim

Use this command to enable debugging for PIM.

Use the no option with this command to deactivate debugging for PIM.

Command Syntax

```
debug ipv6 pim (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state|timer)
debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state
  |timer)
no debug ipv6 pim (all|events|mfc|mib|mtracenexthop|nsm|packet|state|timer)
no debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtracenexthop|nsm|packet
  |state|timer)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
all	Enable debugging for all PIM events
events	Enable debugging for general configuration, Virtual Routing (VR), and VRF context
mfc	Enable debugging for MFC updates
mib	Enable debugging for MIB entries
mtrace	Enable debugging for MTRACE messages
nexthop	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
nsm	Enable debugging for NSM
packet	Enable debugging for PIM packets
state	Enable debugging for PIM states
timer	Enable debugging for PIM timers

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ipv6 pim state
```

debug ipv6 pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the no option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax

```
debug ipv6 pim packet
debug ipv6 pim packet in
debug ipv6 pim packet out
debug ipv6 pim (vrf NAME|) packet
debug ipv6 pim (vrf NAME|) packet in
debug ipv6 pim (vrf NAME|) packet out
no debug ipv6 pim packet
no debug ipv6 pim packet in
no debug ipv6 pim packet out
no debug ipv6 pim (vrf NAME|) packet
no debug ipv6 pim (vrf NAME|) packet in
no debug ipv6 pim (vrf NAME|) packet out
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
in	Debug incoming packets
out	Debug outgoing packets

Command Mode

Configure and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim packet in
```

debug ipv6 pim timer assert

Use this command to enable debugging of the PIM assert timers.

Use the no option with this command to disable debugging for PIM assert timers.

Command Syntax

```
debug ipv6 pim timer assert
debug ipv6 pim timer assert at
debug ipv6 pim (vrf NAME|) timer assert
debug ipv6 pim (vrf NAME|) timer assert at
no debug ipv6 pim timer assert
no debug ipv6 pim timer assert at
no debug ipv6 pim (vrf NAME|) timer assert
no debug ipv6 pim (vrf NAME|) timer assert at
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`at`	Use this option to turn on or turn off debugging of the PIM Assert Timer

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ipv6 pim timer assert at
```

debug ipv6 pim timer bsr

Use this command to enable debugging of the PIM BSR time.

Use the no option with this command to disable debugging of the PIM BSR timer.

Command Syntax

```
debug ipv6 pim timer bsr
debug ipv6 pim timer bsr bst
debug ipv6 pim timer bsr crp
debug ipv6 pim (vrf NAME|) timer bsr
debug ipv6 pim (vrf NAME|) timer bsr bst
debug ipv6 pim (vrf NAME|) timer bsr crp
no debug ipv6 pim timer bsr
no debug ipv6 pim timer bsr bst
no debug ipv6 pim timer bsr crp
no debug ipv6 pim (vrf NAME|) timer bsr
no debug ipv6 pim (vrf NAME|) timer bsr bst
no debug ipv6 pim (vrf NAME|) timer bsr crp
```

Parameters

bst	Turn on or turn off the bootstrap debugging timer
crp	Turn on or turn off the Candidate-RP debugging timer
vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim timer bsr bst
```

debug ipv6 pim timer hello

Use this command to enable debugging of various PIM Hello timers.

Use the no option with this command to disable debugging of the PIM Hello timers.

Command Syntax

```
debug ipv6 pim timer hello
debug ipv6 pim timer hello ht
debug ipv6 pim timer hello nlt
debug ipv6 pim timer hello tht
debug ipv6 pim (vrf NAME|) timer hello
debug ipv6 pim (vrf NAME|) timer hello ht
debug ipv6 pim (vrf NAME|) timer hello nlt
debug ipv6 pim (vrf NAME|) timer hello tht
no debug ipv6 pim timer hello
no debug ipv6 pim timer hello ht
no debug ipv6 pim timer hello nlt
no debug ipv6 pim timer hello tht
no debug ipv6 pim (vrf NAME|) timer hello
no debug ipv6 pim (vrf NAME|) timer hello ht
no debug ipv6 pim (vrf NAME|) timer hello nlt
no debug ipv6 pim (vrf NAME|) timer hello tht
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`ht`	Turn on or turn off the PIM Hello debugging timer (ht)
`nlt`	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
`tht`	Turn on or turn off the Triggered Hello Timer (tht)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim timer hello ht
```

debug ipv6 pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax

```
debug ipv6 pim timer joinprune
debug ipv6 pim timer joinprune et
debug ipv6 pim timer joinprune kat
debug ipv6 pim timer joinprune jt
debug ipv6 pim timer joinprune ot
debug ipv6 pim timer joinprune ppt
debug ipv6 pim (vrf NAME|) timer joinprune
debug ipv6 pim (vrf NAME|) timer joinprune et
debug ipv6 pim (vrf NAME|) timer joinprune kat
debug ipv6 pim (vrf NAME|) timer joinprune jt
debug ipv6 pim (vrf NAME|) timer joinprune ot
debug ipv6 pim (vrf NAME|) timer joinprune ppt
no debug ipv6 pim timer joinprune
no debug ipv6 pim timer joinprune et
no debug ipv6 pim timer joinprune kat
no debug ipv6 pim timer joinprune jt
no debug ipv6 pim timer joinprune ot
no debug ipv6 pim timer joinprune ppt
no debug ipv6 pim (vrf NAME|) timer joinprune
no debug ipv6 pim (vrf NAME|) timer joinprune et
no debug ipv6 pim (vrf NAME|) timer joinprune kat
no debug ipv6 pim (vrf NAME|) timer joinprune jt
no debug ipv6 pim (vrf NAME|) timer joinprune ot
no debug ipv6 pim (vrf NAME|) timer joinprune ppt
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
et	Turn on or turn off the PIM JoinPrune expiry timer (et)
jt	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
kat	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)
ot	Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot)
ppt	Turn on or turn off the f PIM JoinPrune PrunePending Timer ((ppt)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ipv6 pim timer joinprune et
```

debug ipv6 pim timer register

Use this command to enable debugging of the PIM register timer.

Use the no option with this command to disable debugging of the PIM register timer.

Command Syntax

```
debug ipv6 pim timer register
debug ipv6 pim timer register rst
debug ipv6 pim (vrf NAME|) timer register
debug ipv6 pim (vrf NAME|) timer register rst
no debug ipv6 pim timer register
no debug ipv6 pim timer register rst
no debug ipv6 pim (vrf NAME|) timer register
no debug ipv6 pim (vrf NAME|) timer register rst
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
rst	Turn on or turn off the PIM Register Stop Timer (rst)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ipv6 pim timer register
```

ipv6 pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

Use the no option with this command to revert to default.

Command Syntax

```
ipv6 pim accept-register list (<100-199>|<2000-2699>|WORD)
ipv6 pim (vrf NAME|) accept-register list (<100-199>|<2000-2699>|WORD)
no ipv6 pim accept-register
no ipv6 pim (vrf NAME|) accept-register
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<100-199>`	An IP extended access-list value
`<2000-2699>`	An IP extended access-list value in the expanded range
`WORD`	Name of a standard access list

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim accept-register list 121

(config)#no ipv6 pim accept-register
```

ipv6 pim anycast-rp

Use this command to configure an Anycast-RP in the RP set.

Use the no option with this command to remove the Anycast-RP configuration.

Command Syntax

```
ipv6 pim anycast-rp X:X::X:X X:X::X:X
ipv6 pim (vrf NAME|) anycast-rp X:X::X:X X:X::X:X
no ipv6 pim anycast-rp X:X::X:X
no ipv6 pim anycast-rp X:X::X:X X:X::X:X
no ipv6 pim (vrf NAME|) anycast-rp X:X::X:X
no ipv6 pim (vrf NAME|) anycast-rp X:X::X:X X:X::X:X
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`X:X::X:X`	Unicast IPv6 address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
`X:X::X:X`	Destination IPv6 address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

ipv6 pim bind ecmp-bundle

Use this command to bind interfaces to an ECMP Bundles.

Use the no option with this command to unbind the interfaces from an ECMP Bundles

Command Syntax

```
ipv6 pim bind ecmp-bundle WORD
no ipv6 pim bind ecmp-bundle WORD
```

Parameter

WORD	ECMP bundle name

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 pim bind ecmp-bundle ebund1

(config-if)#no ipv6 pim bind ecmp-bundle ebund1
```

ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

When this command is configured on an interface, no PIM Version 2 BSR messages are sent or received through the interface. Use this command to configure an interface bordering another PIM domain to avoid the exchange of BSR messages between the two domains. BSR messages should not be exchanged between different domains because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in a protocol malfunction or loss of isolation between the domains.

Use the `no` option with this command to remove the BSR border configuration.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Command Syntax

```
ipv6 pim bsr-border
no ipv6 pim bsr-border
```

Parameters

None

Default

Bootstrap router border configuration is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures the interface to be the PIM domain border:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim bsr-border

(config)#interface eth0
(config-if)#no ipv6 pim bsr-border
```

ipv6 pim bsr-candidate

Use this command to give the router the candidate BSR status using the name the interface.

Use the no option with this command to disable this function.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message candidate

Command Syntax

```
ipv6 pim bsr-candidate IFNAME
ipv6 pim bsr-candidate IFNAME <0-32>
ipv6 pim bsr-candidate IFNAME <0-32> <0-255>
ipv6 pim (vrf NAME|) bsr-candidate IFNAME
ipv6 pim (vrf NAME|) bsr-candidate IFNAME <0-32>
ipv6 pim (vrf NAME|) bsr-candidate IFNAME <0-32> <0-255>
no ipv6 pim bsr-candidate (IFNAME|)
no ipv6 pim (vrf NAME|) bsr-candidate (IFNAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
IFNAME	Specify the name of the interface
<0-32>	Specify a hash mask length for RP selection
<0-255>	Specify a priority for a BSR candidate

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim bsr-candidate eth0 20 30
```

ipv6 pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to revert to the default settings.

Command Syntax

```
ipv6 pim cisco-register-checksum
ipv6 pim cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD)
ipv6 pim (vrf NAME|) cisco-register-checksum
ipv6 pim (vrf NAME|) cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD)
no ipv6 pim cisco-register-checksum
no ipv6 pim cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD)
no ipv6 pim (vrf NAME|) cisco-register-checksum
no ipv6 pim (vrf NAME|) cisco-register-checksum group-list (<1-99>|<1300-
  1999>|WORD)
```

Parameters

vrf	The VPN routing/forwarding instance.
NAME	Specify the name of the VPN routing/forwarding instance.
group-list	Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.
<1-99>	Specify an IP standard access-list.
<1300-1999>	Specify an IP access-list (expanded range).
WORD	IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim cisco-register-checksum

(config)#ipv6 pim cisco-register-checksum group-list G1
(config)#ipv6 access-list filter permit ff1e:10/128
```

ipv6 pim crp-cisco-prefix

Use this command to turn on or turn the Candidate-RP debugging timerworking with Cisco BSR.

Use the no form of this command to turn off the Candidate-RP debugging timerworking with Cisco BSR.

Command Syntax

```
ipv6 pim crp-cisco-prefix
no ipv6 pim crp-cisco-prefix
```

Parameters

`crp-cisco-prefix`

Candidate-RP debugging timerworking with Cisco BSR.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim crp-cisco-prefix

(config)#noipv6 pim crp-cisco-prefix
```

ipv6 pim

Use this command to enable IPv6 PIM dense-mode or sparse-mode or sparse-dense-mode on the current interface.

Use the no option with this command to disable IPv6 PIM dense-mode or sparse-mode or sparse-dense-mode on the interface.

Command Syntax

```
ipv6 pim (dense-mode|sparse-mode|sparse-dense-mode)
no ipv6 pim (dense-mode|sparse-mode|sparse-dense-mode)
```

Parameters

dense-mode	Enable IPv6 PIM dense-mode operation
sparse-mode	Enable IPv6 PIM sparse-mode operation
sparse-dense-mode	Enable IPv6 PIM sparse-dense-mode operation

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dense-mode

(config)#interface eth0
(config-if)#no ipv6 pim dense-mode

(config)#interface eth0
(config-if)#ipv6 pim sparse-dense-mode

(config-if)#no ipv6 pim sparse-dense-mode
```

ipv6 pim passive

Use this command to enable or disable passive mode operation for local members on the interface. Passive mode essentially stops PIM transactions on the interface, allowing only the Internet Group Management Protocol (IGMP) mechanism to be active.

Use the no option with this command to disable the passive mode.

Command Syntax

```
ipv6 pim (dense-mode|sparse-mode) passive
no ipv6 pim (dense-mode|sparse-mode) passive
```

Parameters

`dense-mode`	Enable passive operation for PIM dense-mode
`sparse-mode`	Enable passive operation for PIM sparse-mode

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dense-mode passive

(config)#interface eth0
(config-if)#no ipv6 pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim sparse-mode passive

(config)#interface eth0
(config-if)#no ipv6 pim sparse-mode passive
```

ipv6 pim dense-group

Use this command to force a particular group to always follow dense mode irrespective of whether RP mapping is available in SM-DM mode.

Use the no option with this command to delete the group-address and follow SM-DM rules.

Command Syntax

```
ipv6 pim dense-group A.B.C.D
ipv6 pim (vrf NAME|) dense-group A.B.C.D
no ipv6 pim dense-group A.B.C.D
no ipv6 pim (vrf NAME|) dense-group A.B.C.D
```

Parameter

A.B.C.D	Specify IP address
NAME	Specify the name of the VRF

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 pim dense-group 1ffe:11::11:11

(config-if)# no ip pim dense-group 1ffe:1::11:11
```

ipv6 pim dr-priority

Use this command to set the designated router's priority value.

Use the no option with this command to remove the priority from the DR.

Command Syntax

```
ipv6 pim dr-priority <0-4294967294>
no ipv6 pim dr-priority (<0-4294967294>|)
```

Parameter

`<0-4294967294>` Valid range of values for DR priority, with a higher value resulting in a higher preference

Default

The default DR priority value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dr-priority 11234

(config)#interface eth0
(config-if)#no ipv6 pim dr-priority 11234
```

ipv6 pim ecmp-bundle

Use this command to create an ECMP bundle.

Use the no option with this command to delete an ECMP bundle.

Command Syntax

```
ipv6 pim ecmp-bundle WORD
ipv6 pim (vrf NAME|) ecmp-bundle WORD
ipv6 pim ecmp-bundle WORD
no ipv6 pim (vrf NAME|) ecmp-bundle WORD
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
WORD	ECMP bundle name

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim exmp-bundle ebund1

(config)#no ipv6 pim ecmp-bundle ebund1
```

ipv6 pim rp embedded

Use this command to embed the PIM Rendezvous Point.

Use the no option with this command to remove the Rendezvous Point.

Command Syntax

```
ipv6 pim rp embedded
no ipv6 pim rp embedded
```

Parameter

embedded	Embed the Rendezvous Point

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim rp embedded

(config)#no ipv6 pim rp embedded
```

ipv6 pim exclude-genid

Use this command to exclude the GenID (generated ID) option from Hello packets sent by the PIM module on an interface.This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to restore PIM its default setting.

Command Syntax

```
ipv6 pim exclude-genid
no ipv6 pim exclude-genid
```

Parameters

None

Default

By default, this command is disabled; that is, the GenID option is included.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim exclude-genid

(config)#interface eth0
(config-if)#no ipv6 pim exclude-genid
```

ipv6 pim hello-holdtime

Use this command to configure a hello holdtime other than the default(`3.5 * hello_interval` seconds).

When configuring `hello-holdtime`, if the configured value is less than the current `hello_interval`, it is refused.

When removing a configured `hello_holdtime`, the value is reset to (`3.5 *` current `hello_interval`) value.

Every time the hello_interval is updated, the hello-holdtime is also updated according to rules below:

If the hello_holdtime is not configured, or if the hello_holdtime is configured, but is less than the current hello_interval value, it is modified to (3.5 * hello_interval). Otherwise, the configured value is maintained.

Use the no option with this command to remove the configured hello-holdtime.

Command Syntax

```
ipv6 pim hello-holdtime <1-65535>
no ipv6 pim hello-holdtime
```

Parameter

`<1-65535>`	Range of values for hello-holdtime, in seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface fxp0
(config-if)#ipv6 pim hello-holdtime 123

(config)#interface fxp0
(config-if)#no ipv6 pim hello-holdtime
```

ipv6 pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the no option with this command to reset the hello-interval to its default value.

Command Syntax

```
ipv6 pim hello-interval <1-65535>
no ipv6 pim hello-interval
```

Parameter

<1-65535>	Range of values for the hello-interval

Note: No fractional values are allowed.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim hello-interval 123

(config)#interface eth0
(config-if)#no ipv6 pim hello-interval
```

ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to remove this setting.

Command Syntax

```
ipv6 pim ignore-rp-set-priority
ipv6 pim (vrf NAME|) ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority
no ipv6 pim (vrf NAME|) ignore-rp-set-priority
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim ignore-rp-set-priority

#configure terminal
(config)#no ipv6 pim ignore-rp-set-priority
```

ipv6 pim jp-timer

Use this command to set a PIM join/prune timer.

Use the no option with this command to remove the join/prune timer.

Command Syntax

```
ipv6 pim jp-timer <1-65535>
ipv6 pim (vrf NAME|) jp-timer <1-65535>
no ipv6 pim jp-timer
no ipv6 pim jp-timer <1-65535>
no ipv6 pim (vrf NAME|) jp-timer
no ipv6 pim (vrf NAME|) jp-timer <1-65535>
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for the Join/Prune timer, in seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim jp-timer 234

#configure terminal
(config)#no ipv6 pim jp-timer 234
```

ipv6 pim neighbor-filter

Use this command to enable filtering of neighbors on the interface.

When configuring a neighbor filter and when denied by filtering access list, PIM either does not establish adjacency with a neighbor or terminates adjacency with existing neighbors.

Use the no option with this command to disable filtering of neighbors on the interface.

Command Syntax

```
ipv6 pim neighbor-filter (<1-99>|WORD)
no ipv6 pim neighbor-filter (<1-99>|WORD)
```

Parameters

<1-99>	An IP standard access-list number
WORD	Name of an IP standard access list

Command Mode

Interface mode

Default

This command is disabled; by default, there is no filtering.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface fxp0
(config-if)#ipv6 pim neighbor-filter F1
(config-if)#exit
(config)#ipv6 access-list filter deny fe80:20e:cff:fe01:facc
(config)#ipv6 access-list filter permit any
```

ipv6 pim propagation-delay

Use this command to configure the propagation delay value.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax

```
ipv6 pim propagation-delay <1000-5000>
no ipv6 pim propagation-delay
```

Parameter

<1000-5000>	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 500 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ipv6 pim propagation-delay
```

ipv6 pim register-rate-limit

Use this command to configure the rate of Register packets sent by this designated router (DR), in number of packets per second.

Use the no option to remove the register-rate-limit configuration.

Note: The configured rate is per (S,G) state, and is not a system-wide rate.

Command Syntax

```
ipv6 pim register-rate-limit <1-65535>
ipv6 pim (vrf NAME|) register-rate-limit <1-65535>
no ipv6 pim register-rate-limit
no ipv6 pim (vrf NAME|) register-rate-limit
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for packets to send per second

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim register-rate-limit 3444

#configure terminal
(config)#no ipv6 pim register-rate-limit
```

ipv6 pim register-rp-reachability

Use this command to enable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to the default state.

Command Syntax

```
ipv6 pim register-rp-reachability
ipv6 pim (vrf NAME|) register-rp-reachability
no ipv6 pim register-rp-reachability
no ipv6 pim (vrf NAME|) register-rp-reachability
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Configure mode

Default

The default setting is no checking for rendezvous point reachability,

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim register-rp-reachability
```

ipv6 pim register-source

Use this command to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the no option to remove the source address of register packets sent by this DR, and reset it to use the default source address, that is, the address of the RPF interface toward the source host.

The configured address must be a reachable address so the RP can send corresponding Register-Stop messages in response. This address is usually the loopback interface address, but can also be other physical addresses. The address must be advertised by unicast routing protocols on the DR.

Note: The interface configured does not require PIM to be enabled.

Command Syntax

```
ipv6 pim register-source IFNAME
ipv6 pim register-source X:X::X:X
ipv6 pim (vrf NAME|) register-source IFNAME
ipv6 pim (vrf NAME|) register-source X:X::X:X
no ipv6 pim register-source
no ipv6 pim (vrf NAME|) register-source
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
X:X::X:X	The IP address to be used as the source of the register packets
IFNAME	The name of the interface to be used as the source of the register packets

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim register-source 3ffe:406::1

#configure terminal
(config)#no ipv6 pim register-source
```

ipv6 pim register-suppression

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR; configuring this value at the RP modifies the RP-keepalive-period value if the `ipv6 pim rp-register-kat` command is not used.

Use the no option to remove the register-suppression setting.

Command Syntax

```
ipv6 pim register-suppression <1-65535>
ipv6 pim (vrf NAME|) register-suppression <1-65535>
no ipv6 pim register-suppression
no ipv6 pim (vrf NAME|) register-suppression
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Register suppression time, in seconds

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim register-suppression 555

#configure terminal
(config)#no ipv6 pim register-suppression
```

ipv6 pim router-id

Use this command to configure PIM router-ID to uniquely identify the router.By default, PIM registers for the NSM router-id service. This command will override the router-id received from NSM.

Use the `no` option with this command to unconfigure PIM router-ID. This will make PIM fall back to the NSM router-id

Command Syntax

```
ipv6 pim (vrf NAME|) router-id A.B.C.D
no ipv6 pim (vrf NAME|) router-id A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	Specify the Router ID

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim router-id 1.1.1.1

(config)#no ipv6 pim router-id 1.1.1.1
```

ipv6 pim rp-address

Use this command to statically configure an RP address for multicast groups.

Use the `no` option to remove the RP address.

OcNOS PIMv6 supports multiple static RPs. It also supports usage of static-RP and BSR mechanism simultaneously. The following list states the correct usage of this command:

- To support embedded RP, the router configured as the RP must use a configured access-list that permits the embedded RP group ranges derived from the embedded RP address. If embedded RP support is available, only the RP must be statically configured as the RP for the embedded RP ranges – no additional configuration is required on other PIMv6 routers. The other routers will discover the RP address from the IPv6 group address. For these routers to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP, and embedded RP support must be disabled.
- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen over statically configured RP-address.
- A single static-RP can be configured for multiple group ranges using Access Lists. However, configuring multiple static RPs (using `ipv6 pim rp-address` command) with the same RP address is not allowed. The static-RP can be configured either for the whole multicast group range `ff00::/8` (without ACL) or for specific group ranges (using ACL).

  For example, configuring `ipv6 pim rp-address 3ffe:10:10:5::153` will configure static-RP `3ffe:10:10:5::153` for the default group range `ff00::/8`. Configuring `ipv6 pim rp-address 3ffe:20:20:5::153 grp-list` will configure static-RP `3ffe:20:20:5::153` for all the group ranges represented by `permit` filters in `grp-list` ACL.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
- Only `permit` filters in ACL are considered as valid group ranges. The default `permit` filter `::/0` is converted to default multicast filter `ff00::/8`.
- When selecting static-RPs for a group range, the first element, with static-RP with the highest IP address is chosen.
- Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ipv6 pim rp-address` command without the `override` keyword. Commands with the `override` keyword take precedence over dynamically learned mappings.

Command Syntax

```
ipv6 pim rp-address X:X::X:X (override|)
ipv6 pim rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)(override|)
ipv6 pim (vrf NAME|) rp-address X:X::X:X (override|)
ipv6 pim (vrf NAME|) rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)(override|)
no ipv6 pim rp-address X:X::X:X
no ipv6 pim rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)
no ipv6 pim (vrf NAME|) rp-address X:X::X:X
no ipv6 pim (vrf NAME|) rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

X:X::X:X	IPv6 address for the RP
<1-99>	An IP Standard access-list
<1300-1999>	An IP Standard access-list (expanded range)
WORD	Access-list name
override	Static RP overrides dynamically-learned RP

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim rp-address 30:30:5::153 4

#configure terminal
(config)#no ipv6 pim rp-address 30:30:5::153 4
```

ipv6 pim rp-candidate

Use this command to give the router a candidate RP status using the IPv6 address of the specified interface.

Additionally, the groups specified will operate in PIM sparse mode; group-list specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address.

Use the no option along with this command to remove the settings.

Command Syntax

```
ipv6 pim (vrf NAME) rp-candidate IFNAME(group-list(<1-99>|WORD))|)(interval <1-
  16383>|) (priority <0-255>|)
no ipv6 pim (vrf NAME) rp-candidate (IFNAME|)
```

Parameters

vrf NAME	The VPN routing/forwarding instance
IFNAME	Specify an interface name
<1-99>	An IP Standard access-list
WORD	A named standard access list
<0-16383>	Range of values for candidate-RP advertisement interval, in seconds
<0-255>	Range of values for priority of an RP candidate

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim rp-candidate eth3

(config)#no ipv6 pim rp-candidate eth3
```

ipv6 pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value.

Use the no option to remove this configuration.

Command Syntax

```
ipv6 pim rp-register-kat <1-65535>
ipv6 pim (vrf NAME|) rp-register-kat <1-65535>
no ipv6 pim rp-register-kat
no ipv6 pim (vrf NAME|) rp-register-kat
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for a KAT time in seconds

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim rp-register-kat 3454

(config)#no ipv6 pim rp-register-kat
```

ipv6 pim spt-threshold

Use this command to configure an SPT (System Posture Token) threshold.

Use the no option with this command to remove a configured SPT threshold.

Note: This option is binary, meaning that switching to SPT happens either the first data packet is received, or not at all. It is not rate-based.

Command Syntax

```
ipv6 pim spt-threshold
ipv6 pim spt-threshold group-list (<1-99>|<1300-1999>|WORD)
ipv6 pim (vrf NAME|) spt-threshold
ipv6 pim (vrf NAME|) spt-threshold group-list (<1-99>|<1300-1999>|WORD)
no ipv6 pim spt-threshold
no ipv6 pim spt-threshold group-list (<1-99>|<1300-1999>|WORD)
no ipv6 pim (vrf NAME|) spt-threshold
no ipv6 pim (vrf NAME|) spt-threshold group-list (<1-99>|<1300-1999>|WORD)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
group-list	Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list
<1-99>	An IP Standard access-list
<1300-1999>	An IP Standard access-list (expanded range)
WORD	A named standard access list

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim spt-threshold group-list LIST1

#configure terminal
(config)#no ipv6 pim spt-threshold
```

ipv6 pim ssm

Use this command to configure Source Specific Multicast (SSM), and define a range of IP multicast addresses. The `default` keyword defines the SSM range as ff3x::/32. To define a SSM range other than the default, specify an access-list.

When an SSM range of IP multicast addresses is defined with this command, the no (*,G) or (S,G,rpt) state is initiated for groups in the SSM range.

The messages corresponding to these states are not accepted or originated in the SSM range.

Use the `no` form of this command to disable the SSM range.

Command Syntax

```
ipv6 pim ssm default
ipv6 pim ssm range (<1-99>|WORD)
ipv6 pim (vrf NAME|) ssm default
ipv6 pim (vrf NAME|) ssm range (<1-99>|WORD)
no ipv6 pim ssm
no ipv6 pim (vrf NAME|) ssm
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`default`	Defines the FF3x::/32 group range for SSM
`range`	Define an access-list for group range to use for SSM
`<1-99>`	Range of values for a standard access-list
`WORD`	A named standard access list

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ipv6 pim ssm range 4
```

ipv6 pim state-refresh origination-interval

Use this command to configure a PIM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM State Refresh control messages.

Use the no option with this command to return the origination interval to its default value.

Command Syntax

```
ipv6 pim state-refresh origination-interval <1-100>
no ipv6 pim state-refresh origination-interval
```

Parameter

<1-100>	Range of values for state-refresh origination interval, in seconds

Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ipv6 pim state-refresh origination-interval
```

ipv6 pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the no option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax

```
ipv6 pim unicast-bsm
no ipv6 pim unicast-bsm
```

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim unicast-bsm

(config)#interface eth0
(config-if)#no ipv6 pim unicast-bsm
```

show debugging ipv6 pim

Use this command to display the debug status for the IPv6 PIM process.

Command Syntax

```
show debugging ipv6 pim
show debugging ipv6 pim (vrf NAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
# show debugging ipv6 pim
PIMv6 Debugging status:
  PIMv6 event debugging is on
  PIMv6 MFC debugging is on
  PIMv6 state debugging is on
  PIMv6 incoming packet debugging is on
  PIMv6 outgoing packet debugging is on
  PIMv6 Hello HT timer debugging is on
  PIMv6 Hello NLT timer debugging is on
  PIMv6 Hello THT timer debugging is on
  PIMv6 Join/Prune JT timer debugging is on
  PIMv6 Join/Prune ET timer debugging is on
  PIMv6 Join/Prune PPT timer debugging is on
  PIMv6 Join/Prune KAT timer debugging is on
  PIMv6 Join/Prune OT timer debugging is on
  PIMv6 Assert AT timer debugging is on
  PIMv6 Register RST timer debugging is on
  PIMv6 Bootstrap BST timer debugging is on
  PIMv6 Bootstrap CRP timer debugging is on
  PIMv6 mib debugging is on
  PIMv6 nexthop debugging is on
  PIMv6 mtrace debugging is on
  PIMv6 NSM debugging is on
  PIMv6 MSDP debugging is on
```

show ipv6 pim interface

Use this command to display information about interfaces configured for PIM.

Command Syntax

```
show ipv6 pim interface
show ipv6 pim interface detail
show ipv6 pim (vrf NAME|) interface
show ipv6 pim (vrf NAME|) interface detail
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`detail`	Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show  ipv6  pim interface detail
eth1 (vif 0):
  Address fe80::5054:ff:fe14:857, DR fe80::5054:ff:fe14:857
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.1 Local-ID 3
  Secondary addresses:
   3ffe:192:168:10::53
  Neighbors:

eth2 (vif 2):
  Address fe80::5054:ff:fe52:219e, DR fe80::5054:ff:fe63:c0ae
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.1 Local-ID 4
  ECMP REDIRECT, bundle : bundle1, status :  allowed
  Secondary addresses:
   3ffe:192:168:1::53
  Neighbors:
   fe80::5054:ff:fe21:5e56
   fe80::5054:ff:fe29:f7f3
   fe80::5054:ff:fe63:c0ae
```

Table 2-44 explains the fields for each pim entry.

Table 2-44: show ipv6 pim interface detail

Entry	Description
Interface name	As stated
Address	The IPv6 address of the interface.
DR	The IPv6 address of the Designated Router (DR).
Hello period	When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages MUST be sent every Hello_Period seconds. The Hello Timer should not be reset except when it expires.
Next Hello	The time period before the next Hello is sent.
Triggered Hello period	A per-interface Hello Timer (HT(I)) is used to trigger sending Hello messages on each active interface. When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay.
Propagation delay	The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message.
ECMP REDIRECT	Whether Equal-Cost Multiple-Path (ECMP) is allowed and on which bundle.
Secondary address	As stated.
Neighbors	The IPv6 addresses of known Multicast neighbors.

show ipv6 pim mroute

Use this command to display information the IPv6 multicast routing table, or the IPv6 multicast routing table based on the specified address or addresses.

Command Syntax

```
show ipv6 pim mroute (detail|)
show ipv6 pim mroute X:X::X:X (detail|)
show ipv6 pim mroute X:X::X:X X:X::X:X (detail|)
show ipv6 pim (vrf NAME|) mroute (detail|)
show ipv6 pim (vrf NAME|) mroute X:X::X:X (detail|)
show ipv6 pim (vrf NAME|) mroute X:X::X:X X:X::X:X (detail|)
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
X:X::X:X	Display all entries for this group IPv6 address
X:X::X:X	Display all entries for this source IPv6 address
detail	Display detailed PIM multicast routing table information

Note: A group IP address and a source IP address cannot be used simultaneously.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 pim mroute

IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 1

(*, ff05::2)
RP: 3ffe:192:168:1::53
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     i.i.............................
 Joined    j.............................
 Asserted  ..............................
FCR:
```

```
(*, ff1e::10)
RP: 3ffe:192:168:1::53
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    ..j...........................
 Asserted  ..............................
FCR:
Source: 3ffe:172:31:1::96
 Outgoing  ..o...........................
 KAT timer running, 207 seconds remaining
 Packet count 1

(3ffe:172:31:1::96, ff1e::10)
RPF nbr: fe80::202:a5ff:fe4f:1073
RPF idx: eth3
SPT bit: 0
Upstream State: JOINED
 Local     ..............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o...........................

(3ffe:172:31:1::96, ff1e::10, rpt)
RP: 3ffe:192:168:1::53
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..............................
#
```

Table 2-45 explains the fields for each pim entry.

Table 2-45: show ipv6 pim mroute

Entries	Description
(*,*,RP) Entries	Optional (*,*,RP) (RFC 4601), PIM Multicast Border Router feature and authentication using IPsec that lack sufficient deployment experience. this is obsoleted by RFC 7761.
(*,G) Entries	A wild card Group entry for all sources within group G.
(S,G) Entries	Source Specific to a Group. IGMPv3 permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source.
(S, G, rpt) Entries	Source Specific to a Group and Rendezvous Point Tree entries.
RP	Rendezvous Point address

Table 2-45: (Continued)show ipv6 pim mroute

Entries	Description
RPF nbr	“Reverse Path Forwarding Neighbor” address. The RPF Neighbor of a router with respect to an address is the neighbor that the MRIB indicates should be used to forward packets to that address.
RPF idx	RPF interface (RP) is the interface the MRIB indicates would be used to route packets to the RP, except at the RP when it is the decapsulation interface (the “virtual” interface on which Register packets are received).
SPT bit	The SPT bit is used to indicate whether forwarding is taking place on the (S,G) Shortest Path Tree (SPT) or on the (*,G) tree.
Upstream State	The state of the a particular entry. States are: Local, Joined, Pruned Not Pruned, Asserted, or Outgoing.
KAT timer running	Keep Alive Timer.
Source	The Source address.

show ipv6 pim neighbor

Use this command to display IPv6 PIM neighbor information.

Command Syntax

```
show ipv6 pim neighbor (detail|)
show ipv6 pim neighbor IFNAME (detail|)
show ipv6 pim neighbor IFNAME X:X::X:X (detail|)
show ipv6 pim (vrf NAME|) neighbor (detail|)
show ipv6 pim (vrf NAME|) neighbor IFNAME (detail|)
show ipv6 pim (vrf NAME|) neighbor IFNAME X:X::X:X (detail|)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Name of the interface
`X:X::X:X`	IPv6 address of the neighbor interface
`detail`	Display detailed information for a PIM neighbor

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ipv6 pim neighbor detail
rtr6# show  ipv6  pim  neighbor  detail
Nbr fe80::5054:ff:fe21:5e56 (eth2)
Expires in 83 seconds, uptime 01:37:14
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 321289676,
Interface ID: Router-ID: 4.4.4.4 Local-ID: 4,
ECMP REDIRECT enabled
Secondary addresses:
  3ffe:192:168:1::150

Nbr fe80::5054:ff:fe29:f7f3 (eth2)
Expires in 79 seconds, uptime 01:37:15
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 847253139,
Interface ID: Router-ID: 2.2.2.2 Local-ID: 4,
ECMP REDIRECT enabled
Secondary addresses:
  3ffe:192:168:1::149
```

Table 2-46 explains the fields for each pim entry.

Table 2-46: show ipv6 pim Neighbor

Entry	Description
Interface name	As stated
Address	The IPv6 address of the interface.
DR	The IPv6 address of the Designated Router (DR).
Hello period	When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages MUST be sent every Hello_Period seconds. The Hello Timer should not be reset except when it expires.
Next Hello	The time period before the next Hello is sent.
Triggered Hello period	A per-interface Hello Timer (HT(I)) is used to trigger sending Hello messages on each active interface. When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay.
Propagation delay	The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message.
ECMP REDIRECT	Whether Equal-Cost Multiple-Path (ECMP) is allowed and on which bundle.
Secondary address	As stated.

show ipv6 pim nexthop

Use this command to display the nexthop information from NSM as used by IPv6 PIM.

Command Syntax

```
show ipv6 pim nexthop
show ipv6 pim (vrf NAME|) nexthop
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable
Destination           Type  Nexthop Nexthop Nexthop  Nexthop Metric    Pref
Refcnt
                            Num     Addr    Ifindex  Name
_____________________________________________________________________________
_______
2001:db8:10:5::153    .RS.  1       fe80::20e:cff:fe01:facc  2     30  110
1
```

show ipv6 pim bsr-router

Use this command to show the bootstrap router v2 address.

Command Syntax

```
show ipv6 pim bsr-router
show ipv6 pim (vrf NAME|) bsr-router
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 pim bsr-router
  PIMv2 Bootstrap information
  This system is the Bootstrap Router (BSR)
    BSR address: 3ffe:b00:c18:1::10
    Uptime:      00:37:12, BSR Priority: 64, Hash mask length: 10
    Next bootstrap message in 00:00:04
    Role: Candidate BSR
    State: Elected BSR
    Candidate RP: fe80::5054:ff:fe21:5e56(eth1)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:27
```

Table 2-47 explains the fields for each pim entry.

Table 2-47: show ipv6 pim bsr-router

Entry	Description
BSR address	Address of the Bootstrap router (BSR).
Uptime	As Stated.
BSR Priority	The current priority of the BSR (this is configurable).
Hash mask length	For Rendezvous Point (RP) addresses in the matching group-range-to-RP mappings, compute a value — Value(G,M,C(i))= (1103515245 * ((1103515245 * (G&M)+12345) XOR C(i)) + 12345) mod 2^31 where C(i) is the RP address and M is a hash-mask.
Next bootstrap message	Time until next boostrap message.
Role	AS stated..

Table 2-47: show ipv6 pim bsr-router

Entry	Description
State	As stated..
Candidate RP	Address of the rendezvous point (RP).
Advertisement interval	As stated.
Next C-RP advertisement	Time before the next Candidate RP is advertised.

show ipv6 pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax

```
show ipv6 pim local-members
show ipv6 pim local-members IFNAME
show ipv6 pim (vrf NAME|) local-members
show ipv6 pim (vrf NAME|) local-members IFNAME
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Display neighbors for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 pim local-members
PIM Local membership information

eth1:
  (*, ff05::2) : Include

eth2:
  (*, ff05::2) : Include
  (*, ff1e::10) : Include
#
```

Table 2-48 explains the fields for each pim entry.

Table 2-48: show ipv6 pim local-members output

Entries	Description
Port	Port name
(*, G)	State that maintains the Rendezvous Point for the Group (G).

show ipv6 pim rp-hash

Use this command to display the rendezvous point (RP) based on the group selected.

Command Syntax

```
show ipv6 pim rp-hash X:X::X:X
show ipv6 pim (vrf NAME|) rp-hash X:X::X:X
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
X:X::X:X	Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 pim rp-hash ff1e::10
    RP: 3ffe:192:168:1::57
    Info source: 3ffe:192:168:1::57, via bootstrap
#
```

Table 2-49 explains the fields for each pim entry.

Table 2-49: show ipv6 pim rp-hash

Entries	Description
RP	Address of the Rendezvous Point
Info source	Address of the information source. In this case the information comes from the Bootstrap router.

show ipv6 pim rp mapping

Use this command to display the mappings for the PIM group to the active rendezvous points.

Command Syntax

```
show ipv6 pim rp mapping
show ipv6 pim (vrf NAME|) rp mapping
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ipv6 pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0


Group(s): ff00::/8, Static
    RP: aab1:23::1
         Uptime: 00:05:44
    RP: a121:33::1
         Uptime: 00:00:29
    RP: 3ffe:172:31:12::2
         Uptime: 00:14:54
Embedded RP Groups:
```

undebug all ipv6 pim

Use this command to disable all PIM debugging.

Command Syntax

```
undebug all ipv6 pim
undebug (vrf NAME|) all ipv6 pim
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#undebug all ipv6 pim
```

SECTION 8

Carrier Ethernet

Carrier Ethernet Configuration Guide

Contents

This document contains these chapters and appendices:

CHAPTER 1 Link Layer Discovery Protocol Configuration

This chapter contains a complete sample Link Layer Discovery Protocol (LLDP) configuration.

LLDP is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN, and then to store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device is able to advertise its identity, its capabilities and its media-specific configuration, as well as learn the same information from other connected devices.

Note: The `lldp-agent` command is not supported for SVLAN, VLAN, and loop-back interfaces.

Topology

Figure 1-78 displays a sample LLDP topology.

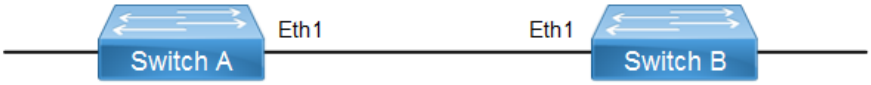


Figure 1-78: LLDP Topology

Interface Mode TLV

Default Agent

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the `port-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the `system-name TLV` to be transmitted on the port

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the `system-capabilities TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the `system-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the `management-address TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the `VLAN-id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the `VLAN-NAME TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the `Port and Protocol VLAN id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the `Protocol Identity TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the `VID Usage Digest TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the `Management VID TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the `Link Aggregation TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLDPDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch

```
#show running-config lldp
!
interface eth1
lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
```

```
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 nearest-bridge

Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 4
  Total entries aged          : 0
  Total frames received       : 3
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Customer Bridge

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent customer-bridge`	Enter into the Customer Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port.

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port.
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods.
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show #show running-config lldp
!
interface eth1
lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
```

```
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 customer-bridge

Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 8
  Total entries aged          : 0
  Total frames received       : 7
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Non-Tpmr-Bridge

The below configurations should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the Non tpmr Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show running-config lldp
lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
```

```
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6

!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 non-tmpr-bridge

Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 17
  Total entries aged          : 0
  Total frames received       : 6
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Media Endpoint Devices TLV

Switch A

`(config)#interface eth1`	Enter interface mode.
`(config-if)#lldp-agent`	Enter the default agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent customer-bridge`	Enter the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter the non-tpmr-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#set lldp med-devtype net-connect`	Enter the med-devtype agent and set the device type to network connectivity.
`(config-if)#exit`	Exit agent mode.

Validation

```
#show run lldp
!
!
interface eth1
 lldp-agent
```

```
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
#

#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 97
  Total entries aged         : 1
  Total frames received      : 92
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 89
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 90
  Total entries aged         : 0
```

```
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
#
```

Switch B

(config)#interface eth1	Enter interface mode.
(config-if)#lldp-agent	Enter the default agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#lldp-agent customer-bridge	Enter the customer-bridge agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#lldp-agent non-tpmr-bridge	Enter the non-tpmr-bridge agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#set lldp med-devtype ep-class3	Enter the med-devtype agent and set the device type to endpoint class 3.
(config-if)#exit	Exit agent mode.

Validation

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 set lldp med-devtype ep-class3
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
!
#

#show lldp interface eth1
Agent Mode                  : Customer-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                : Y
```

```
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 11
  Total entries aged         : 0
  Total frames received      : 12
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 8
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
#
```

Global Mode TLV

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

Topology

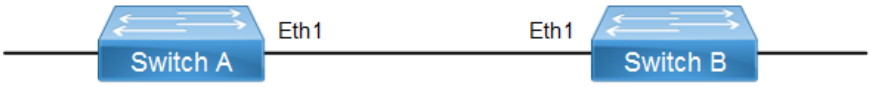


Figure 1-79: LLDP topology

SW1

`SW1#configure terminal`	Enter Configure mode
`SW1(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW1(config)#interface eth1`	Enter interface mode
`SW1(config-if)#lldp-agent`	Enter LLDP interface mode
`SW1(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW1(if-lldp-agent)#exit`	Exit LLDP mode
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#end`	Exit the configure mode

SW2

`SW2#configure terminal`	Enter Configure mode
`SW2(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW2(config)#interface eth1`	Enter interface mode
`SW2(config-if)#lldp-agent`	Enter LLDP interface mode
`SW2(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW2(if-lldp-agent)#exit`	Exit LLDP mode
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#end`	Exit the configure mode

Validation

```
SW1#show running-config lldp
!
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
!
interface eth1
 lldp-agent
  set lldp enable txrx


SW1#show lldp neighbors

Loc PortID      Rem Host Name      Rem Chassis Id     Rem Port Id       Agent Mode

--------------------------------------------------------------------------------
Eth1           OcNOS              cc37.ab56.6d80     cc37.abbb.ed81   Nearest bridge


SW1#show lldp neighbors detail

--------------------------------------------------------------------------------

Nearest bridge Neighbors
Interface Name              : eth1
 Mandatory TLVs
 Chassis id type          : MAC address [cc37.ab56.6d80]
 Port id type             : MAC address [cc37.abbb.ed81]
 Time to live             : 121
 Basic Management TLVs
 System Name              : SW2
 System Description       : Hardware Model:EC_AS4610-54, Software version: Oc
NOS,1.3.6.241a
 Port Description          : eth1
 Remote System Capabilities : Bridge
                              Router
 Capabilities Enabled     : Router
 Management Address        : MAC Address [cc37.abbb.ed81]
 Interface Number subtype  : ifindex
 Interface Number          10046
 OID Number              : 0
 802.1 Org specific TLVs
 Port vlan id              : 0
 Port & Protocol vlan id   : 0
 Remote Configured VLANs   : None
 Remote Protocols Advertised: None
```

```
 Remote VID Usage Digest   : 0
 Remote Management Vlan    : 0
 Link Aggregation Capability: not capable of being aggregated
 Link Aggregation Status   : not currently in aggregation
 Link Aggregation Port ID  :
 802.3 Org specific TLVs
 AutoNego Support          : Not-Supported
 AutoNego Status           : Disabled
 AutoNego Capability       : 0
 Operational MAU Type      : 0 [unknown]
  Max Frame Size            :
SW1#
```

LLDP-MED

LLDP extensions and behavior requirements are described specifically in the areas of network Configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management.

Based on the device type, different TLVs are advertised by the Station.

LLDP-MED Network Connectivity Device

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Configuration Command

```
set lldp med-devtype net-connect
```

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services.

Configuration command:

```
set lldp med-devtype ep-class1
```

LLDP-MED Generic Endpoint (Class 2)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar

Configuration command:

```
set lldp med-devtype ep-class2
```

LLDP-MED Generic Endpoint (Class 3)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Configuration command:

```
set lldp med-devtype ep-class3
```

Switch A

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(if-config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.

`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype net-connect`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

Switch B

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype ep-class3`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations on Switch A:

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
```

2. Verify the LLDP port statistics on Switch A:

```
#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 11
  Total entries aged         : 0
  Total frames received      : 10
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0

#show lldp interface eth1 non-tpmr-bridge
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
```

```
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

3. Verify the LLDP configurations for end device ep-class3 on Switch B:

```
#show running-config lldp
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
!
```

4. Verify the LLDP port statistics on Switch B:

```
#show lldp interface eth1
Agent Mode                  : Customer-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 124
  Total entries aged         : 0
  Total frames received      : 125
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                  : Non-TPMR-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 120
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                  : Nearest bridge
```

```
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 120
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
#
```

CHAPTER 2 Provider Bridging Configuration

This chapter contains sample provider bridging configurations.

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

Single Provider Bridge Configuration

Topology

Figure 2-80: Single provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode customer-edge access`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface

`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PEB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2

SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW3(config-vlan)#exit	Exit VLAN configuration mode
SW3(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW3(config-cvlan-registration)#cvlan 2 svlan 200	Map cvlan2 with svlan 200
SW3(config-cvlan-registration)#exit	Exit registration table
SW3(config)#interface eth1	Enter interface configuration mode for eth1
SW3(config-if)#switchport	Configure switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode customer-edge access	Configure switchport mode customer edge
SW3(config-if)#switchport customer-edge access vlan 2	Associate customer vlan2 with interface
SW3(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW3(config-if)#exit	Exit interface mode
SW3(config-if)#interface eth2	Enter interface configuration mode for eth2
SW3(config-if)#switchport	Make interface as switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#exit	Exit interface configuration mode

Validation

```
SW3#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                200           eth1         0000.0000.0f00    1     300
 1                200           eth2        0001.0000.0800    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                200           eth2         0000.0000.0f00    1     300
 1                200           eth1        0001.0000.0800    1     300

SW1#sh cvlan registration table
```

```
Bridge          Table Name      Port List

======          ==========      =========

1               map1            eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Two Provider Bridge Configuration

Topology

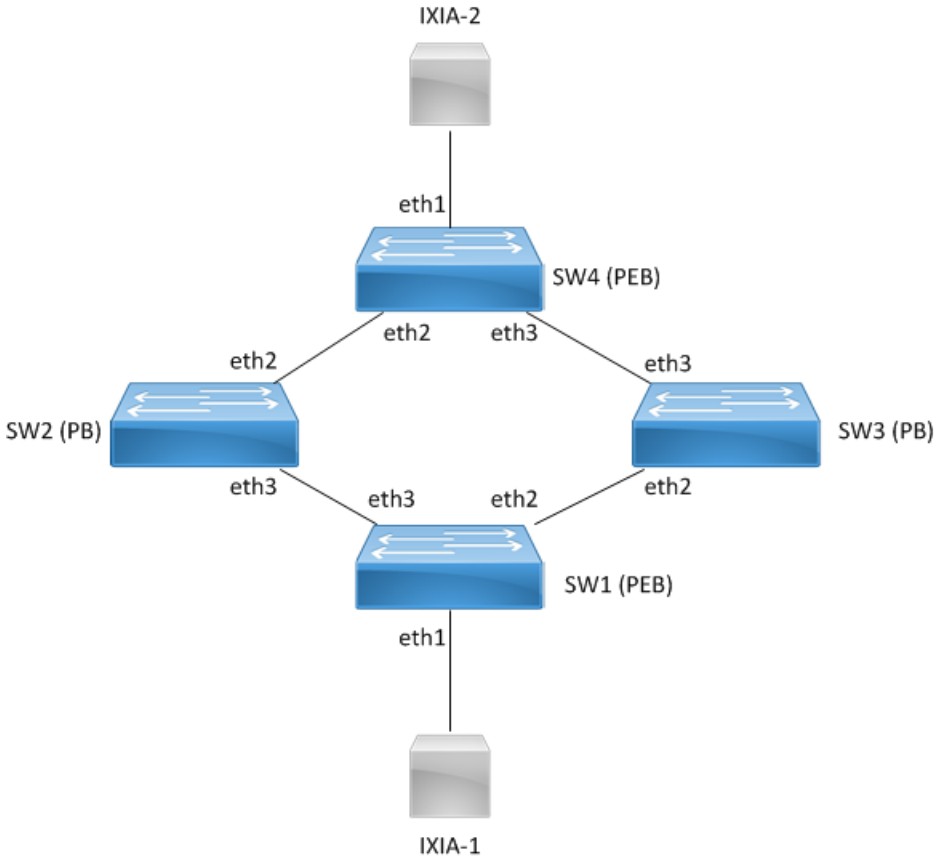


Figure 2-81: Two provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode customer-edge access`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#interface eth3`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth3`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#interface eth3`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#exit`	Exit interface configuration mode
`SW3(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1

SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#exit	Exit interface configuration mode

SW4 (PEB)

SW4#configure terminal	Enter configuration mode
SW4(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW4(config)#vlan database	Enter VLAN configuration mode
SW4(config-vlan)#vlan 2 type customer bridge 1 state enable	Create customer vlan VLAN 2
SW4(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW4(config-vlan)#exit	Exit VLAN configuration mode
SW4(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW4(config-cvlan-registration)#cvlan 2 svlan 200	Map cvlan2 with svlan 200
SW4(config-cvlan-registration)#exit	Exit registration table
SW4(config)#interface eth1	Enter interface configuration mode for eth1
SW4(config-if)#switchport	Configure switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode customer-edge access	Configure switchport mode customer edge
SW4(config-if)#switchport customer-edge access vlan 2	Associate customer vlan2 with interface
SW4(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW4(config-if)#exit	Exit interface mode
SW4(config-if)#interface eth2	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port
SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#interface eth3	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port

SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#exit	Exit interface configuration mode

Validation

```
SW4#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                200           eth1        0000.0000.0a00    1     300
 1                200           eth2        0001.0000.0b00    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                200           eth1        0000.0000.0b00    1     300
 1                200           eth3        0001.0000.0a00    1     300

SW1#sh cvlan registration table
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Layer 2 Protocol Tunneling (L2PT/ L2CP Tunneling)

L2CP tunneling provides support for tunneling Control plane frames between CE nodes.

When control frames received at CEP port of PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is used for tunnelling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunnelled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or updating is done as per registration table / vlan translation table.

Topology

Figure 2-82 displays a sample Provider Bridged topology with customer equipment.

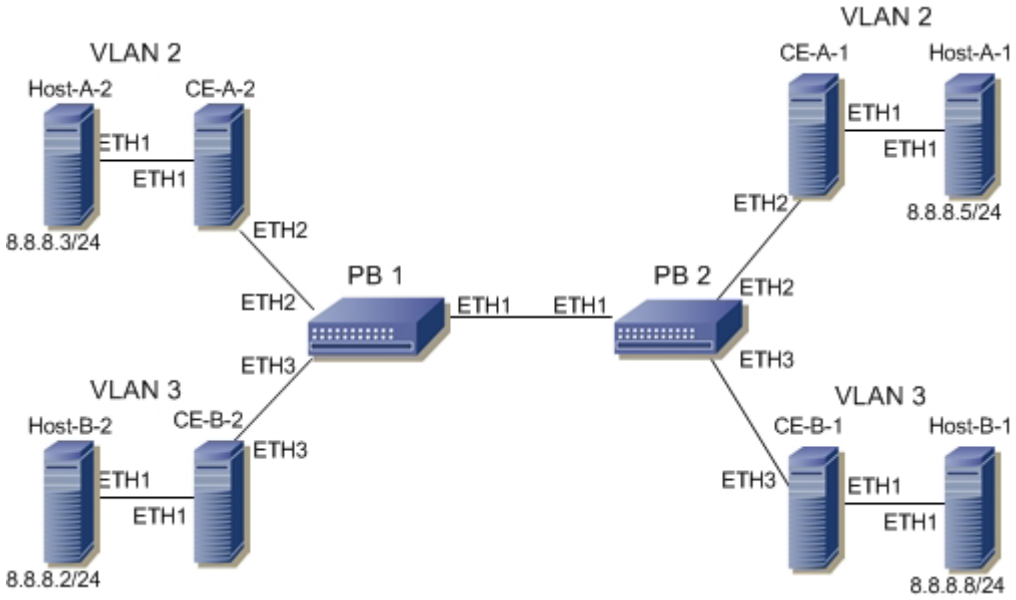


Figure 2-82: Provider Bridging with Customer Equipment Topology

Configuring the L2PT Protocol on the Interface

The following L2PT protocols are supported in OcNOS-SP version 1.0 release:

- efm Ethernet first mile (Link OAM)
- elmi Ethernet local management interface
- lacp Link Aggregation (LACP)
- lldp Link layer discovery protocol
- stp Spanning Tree Protocols
- synce Synchronous Ethernet

PB1

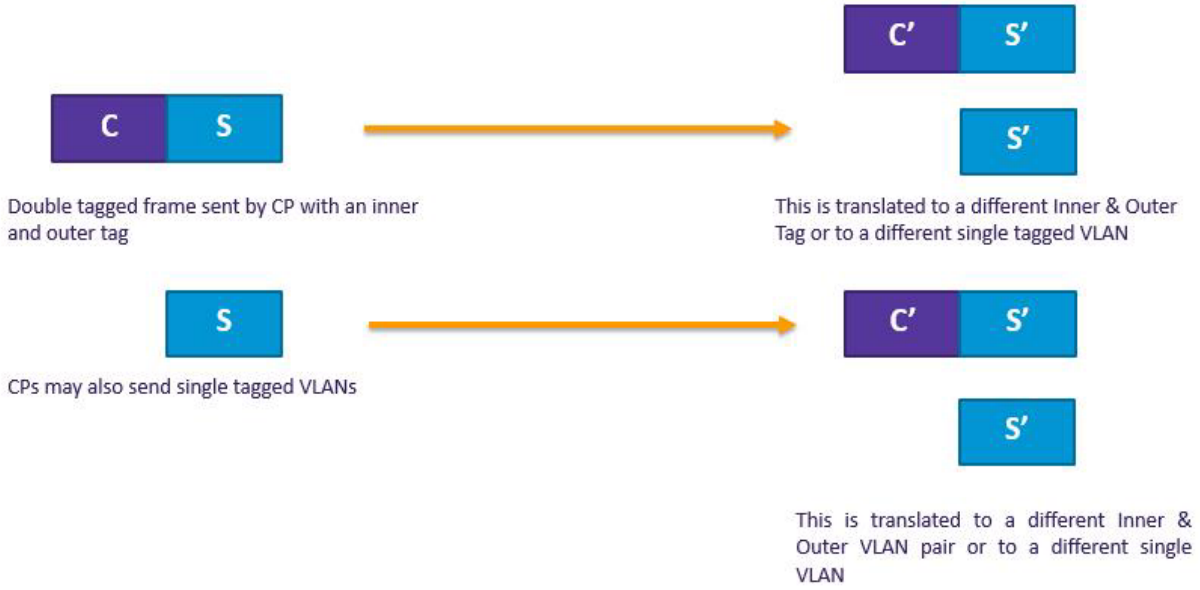
`PB1#configure terminal`	Enter Configure mode.
`PB1(config)#interface eth2`	Enter Interface mode
`PB1(config-if)#l2protocol stp peer`	Configure STP protocol as peer
`PB1(config-if)#l2protocol elmi tunnel`	Configure Elmi protocol as tunnel
`PB1(config-if)#l2protocol lldp tunnel`	Configure LLDP protocol as tunnel
`PB1(config-if)#l2protocol lacp discard`	Configure LACP protocol as discard
`PB1(config-if)#l2protocol efm discard`	Configure EFM protocol as discard
`PB1(config-if)#l2protocol synce discard`	Configure Synce protocol as discard
`PB1(config-if)#exit`	Exit of the interface

Validation

```
PB1#show l2protocol processing interface eth2
Bridge    Interface Name                 Protocol       Processing Status
======    ==============                 ========       =================
1         eth2                           stp            Peer
1         eth2                           gmrp           Peer
1         eth2                           gvrp           Peer
1         eth2                           mmrp           Peer
1         eth2                           mvrp           Peer
1         eth2                           lacp           Discard
1         eth2                           lldp           Tunnel
1         eth2                           efm            Discard
1         eth2                           elmi           Tunnel
1         eth2                            ptp           Peer
1         eth2                           synce          Discard
```

Provider Bridging with VLAN Translation

This is a sample configurations to verify functionality to support provider-bridging feature with extended SVLAN translation as below:



Topology

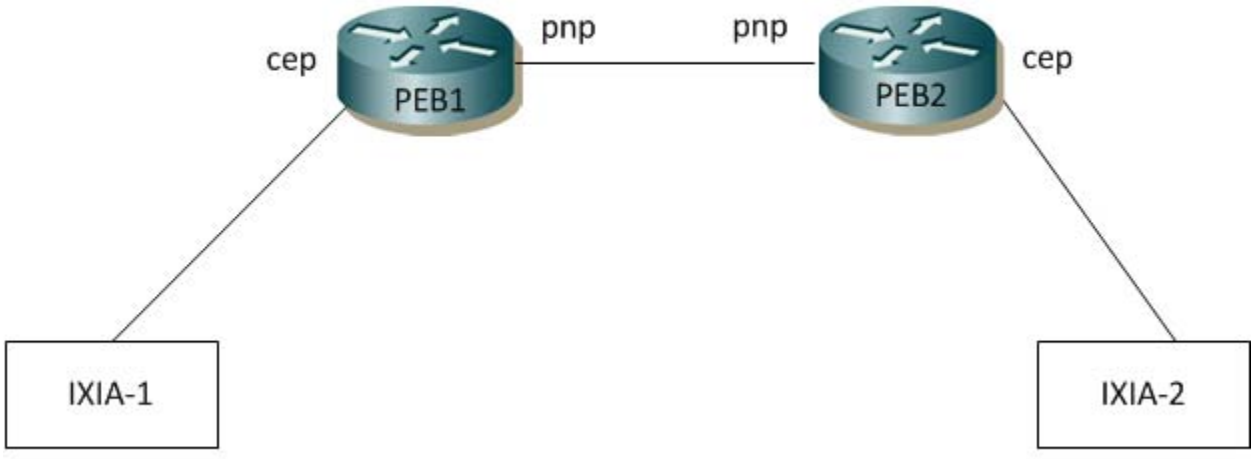


Figure 2-83: Provider Bridging with VLAN Traslation Topology

PEB1

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol provider-rstp edge`	Enter Configure bridge type as provider-RSTP edge bridge
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)# vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode

(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#end	Exit interface and configure mode.

PEB2

Bridge Configuration

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol provider-rstp edge	Enter configure bridge type as provider-RSTP edge bridge
(config)#exit	Exit configure mode.

VLAN Configuration

#configure terminal	Enter configure mode.
(config)#vlan database	Enter VLAN database
(config-vlan)#vlan 2-500 type customer bridge 1 state enable	Configure customer VLANs on bridge 1
(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable	Configure service VLANs on bridge 1
(config-vlan)#end	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

#configure terminal	Enter configure mode.
(config)#cvlan registration table map1 bridge 1	Configure CVLAN registration table as map1
(config-cvlan-registration)#cvlan 2 svlan 6	Map CVLAN to SVLAN
(config-cvlan-registration)#cvlan 3 svlan 7	Map CVLAN to SVLAN
(config-cvlan-registration)#end	End the CVLAN registration mode

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port

`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#end`	Exit interface and configure mode.

Translation Cases

Case1 - (C S - C' S')

Configuration on PEB2

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 cvlan 3 svlan 7`	Translate CVLAN and SVLAN to new CVLAN and new SVLAN on PNP port

Validation for Case 1

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case1.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address     FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1            ge27        1402.ec1c.3144    1     300
 1               6            ge9         6400.6a1e.d9a5    1     300
 1               7            ge9         0000.0500.0400    1     300
 1               7            ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 after translation. Also, captured packets on CEP show new CVLAN 3.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1            ge9         74e6.e2af.598b    1     300
 1               6            ge3         0000.0500.0400    1     300
 1               6            ge9         0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 on provider network from IXIA-2, translation to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case2 - (C S - S')

Configuration on PEB2

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 3`	Allow access VLAN 3 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case1 from PNP port
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 svlan 7`	Configure Translation Case2 on PNP port
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 2

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and translated to new SVLAN as per Case2.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1                 1             ge27        1402.ec1c.3144    1     300
 1                 7             ge9         0000.0500.0400    1     300
```

New SVLAN 7 is observed on PEB2 after translation. At CEP port connected to IXIA-2, untagged traffic should be received.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1.

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1               1             ge9          74e6.e2af.598b     1     300
 1               6             ge3          0000.0500.0400     1     300
 1               6             ge9          0000.0500.0700     1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 from IXIA-2, translatiom to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case3 - (S - S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case2 from PNP port
`(config-if)#switchport provider-network vlan translation svlan 6 svlan 7`	Configure Translation Case3 on PNP port
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 3

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with only STAG entering provider network and translation happens to new SVLAN as per Case3.

```
PEB2#show bridge
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1              1             ge27         1402.ec1c.3144    1     300
 1              6             ge9          0000.0500.0400    1     300
 1              6             ge9          6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 At PNP port connected to IXIA-2.

When double tagged traffic of CVLAN 2 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1              1             ge9          74e6.e2af.598b    1     300
 1              7             ge3          0000.0500.0400    1     300
 1              6             ge9          0000.0500.0700    1     300
```

Here we get a tagged traffic of CVALN 2 when the captured at IXIA-1.

Case4 - (S - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode

`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#no switchport provider-network vlan translation svlan 6`	Unconfigure Translation Case2 from PNP port
`(config-if)#switchport provider-network vlan translation svlan 6 cvlan 3 svlan 7`	Configure Translation Case3 on PNP port
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 4

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 enters provider network and translation happens to new CVLAN and new SVLAN as per Case4.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1              1             ge27        1402.ec1c.3144    1     300
 1              6             ge9         0000.0500.0400    1     300
 1              6             ge9         6400.6a1e.d9a5    1     300
```

When you observe the traffic received in IXIA-2, you can observe that new CVLAN 3 and SVLAN 7 tags can be seen. Here the VLAN 2 will be a data packet.

When tagged traffic for CVLAN 3 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
```

```
1               6               ge3          0000.0500.0400    1      300
1               7               ge9          0000.0500.0700    1      300
```

When you observe, in PEB1 the packets will be dropped at the CEP port since only a single S tagged packets is obtained in the PNP.

Case5 - (C - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 cvlan3 svlan 4`	Map CVLAN to C'VLAN and SVLAN
`(config-cvlan-registration)#cvlan 5 cvlan 6 svlan 7`	Map CVLAN to C'VLAN and SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#end`	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 5

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case1.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1               6             ge9         0000.0500.0400    1     300
 1               6             ge9         6400.6a1e.d9a5    1     300
```

When the packet is captured at PNP port of PEB2 CVLAN of 3 and SVLAN of 4 is seen.

When tagged traffic for CVLAN 6 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
 1               4             ge3         0000.0500.0400    1     300
 1               7             ge9         0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 6 and SVLAN 7 on provider network from IXIA-2, translation to CVLAN 5 and SVLAN 7 happens. Also, captured packets have CVLAN as 2 based on the entry in the cvlan registration table.

Switchport ethertype

Bridge Configuration (for 0x88a8)

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 4`	Map CVLAN to SVLAN

(config-cvlan-registration)#cvlan 3 svlan 6	Map CVLAN to SVLAN
(config-cvlan-registration)#end	End the CVLAN registration mode

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network vlan allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#switchport dot1q ethertype 0x88a8	Change the TPID of the SVLAN to 0x88a8
(config-if)#end	Exit interface and configure mode.

Validation for Switchport ethertype

To validate, send tagged traffic of VLAN 2 from IXIA-1.

Now at eth9 of PB2, capture the packets through IXIA-2 and verify that the traffic is received with double tag.

If the 2 tags CVLAN tag 2 will have the TPID of 0x8100 and SVLAN tag 4 will have a TPID of 0x88a8.

Provider Bridging QoS Configuration

This chapter contains sample provider bridging configurations for QoS.

Scenario: 1 Traffic flow from CEP to PNP

Topology

Figure 2-84: Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 501`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter the interface mode

(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan add 501	Add all VLANs configured above to this PNP port
(config-if)#end	Exit interface and configure mode.

QoS Configurations

#configure terminal	Enter configure mode.
(config)#hardware-profile filter qos-ext enable	Enabling Ingress extended QoS group for QoS support with statistics
(config-if)#qos enable	Enabling QoS
(config-if)#qos statistics	Enabling QoS statistics
(config-if)#qos profile cos-to-queue cosq-cust1	Configure QoS map profile
config-ingress-cos-map)#cos 0 queue 1	Configuring the cos value to be mapped to queue
(config-ingress-cos-map)#exit	Exit configure mode.
(config)#qos profile queue-color-to-cos cosq-service1	Configuring profile for queue color to cos map
(config-egress-cos-map)#queue 1 cos 3	Configuring the queue value to be cos remarked.
(config-egress-cos-map)#exit	Exit configure mode
(config)#cvlan registration table map1 bridge 1	Enter CVLAN registration mode
(config-cvlan-registration)#cvlan 2 svlan 501 cos-to-queue cosq-cust1	Map CVLAN to SVLAN with QoS map profile. Eg: when vlan 2 customer traffic with cos 0 value is received, queue will be assigned to 1 based on mapping.
(config-cvlan-registration)#end	End the CVLAN registration mode
(config)#interface xe3	Enter the interface mode
(config-if)#qos map-profile queue-color-to-cos cosq-service1	Map the profile to the PNP port. Eg: when traffic goes out of queue 1, cos value on service vlan header will be modified to 3 as remarking is enabled on the interface.

(config-if)#qos remark cos enable	Enabling Cos Remark on the Network Interface.
(config-if)#end	Exit interface and configure mode.

Validation for Scenario 1

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-
Cos
========        ==========      ========        ============
=================
2               -               501             cosq-cust1      No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

```
#show qos-profile interface xe3
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: cosq-service1
 profile type: queue-color-to-cos (Egress)
 Status: Active
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |       INPUT      | OUTPUT  |       INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    3       |  1       yellow   3       |  1       red      3
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

Scenario: 2 Traffic flow from PNP to CEP

Topology

Figure 2-85: Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter the interface mode

(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Add all VLANs configured above to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan add 501	Add all VLANs configured above to this PNP port
(config-if)#end	Exit interface and configure mode.

QoS Configurations

#configure terminal	Enter configure mode.
(config)#hardware-profile filter qos-ext enable	Enabling Ingress extended QoS group for QoS support with statistics
(config-if)#qos enable	Enabling QoS
(config-if)#qos statistics	Enabling QoS statistics
(config-if)#qos profile cos-to-queue cosq-cust1	Configure QoS map profile
config-ingress-cos-map)#cos 2 queue 5	Configuring the cos value to be mapped to queue. Eg: when double tagged traffic with cos 2 for outer vlan is received, queue will be assigned to 5 based on mapping.
(config-ingress-cos-map)#exit	Exit configure mode.
(config)#cvlan registration table map1 bridge 1	Enter CVLAN registration mode
(config-cvlan-registration)#cvlan 2 svlan 501 remark-cos	Map CVLAN to SVLAN with remark cos enabled. Eg: when double tagged traffic with cos 2 for outer vlan is received, queue will be assigned to 5 based on mapping and cos value will be changed to 5 when it goes out of cep port since remark cos is enabled.
(config-cvlan-registration)#cvlan 3 svlan 501 remark-cos	Map CVLAN to SVLAN without remark cos. Eg: when double tagged traffic with cos 2 for outer vlan is received, and cos value will be forwarded as it is when it goes out of cep port since remark cos is not enabled for customer2.
(config-cvlan-registration)#end	End the CVLAN registration mode
(config)#configure terminal	Enter configure mode

(config)#interface xe3	Enter the interface mode
(config-if)#qos map-profile cos-to-queue cosq-service	Map the profile to the PNP port
(config-if)#end	Exit interface and configure mode

Validation for Scenario 2

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-
Cos
========        ==========      ========        ============
=================
2               -               501             N/A             Yes
3               -               501             N/A             No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
```

```
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

#show qos-profile interface xe3
profile name: cosq-service
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       5       green    |  2       1       5       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |       INPUT      | OUTPUT  |       INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

CHAPTER 3 Ethernet CFM Configurations

This chapter contains examples of Ethernet Operations and Management (OAM) configurations using the Connectivity Fault Management (CFM) protocol.

Connectivity Fault Management detects, verifies, isolates and notifies connectivity failures on a Virtual Bridged LAN (B-VLAN) based on the protocol standard specified in IEEE 802.1ag 2007. It provides discovery and verification of paths through 802.1 bridges and LANs and is part of the Operation, Administration and Management (OAM) module. CFM is transparent to customer data being transported by a network and is capable of providing maximum fault management.

Continuity Check Message(CCM)

Topology

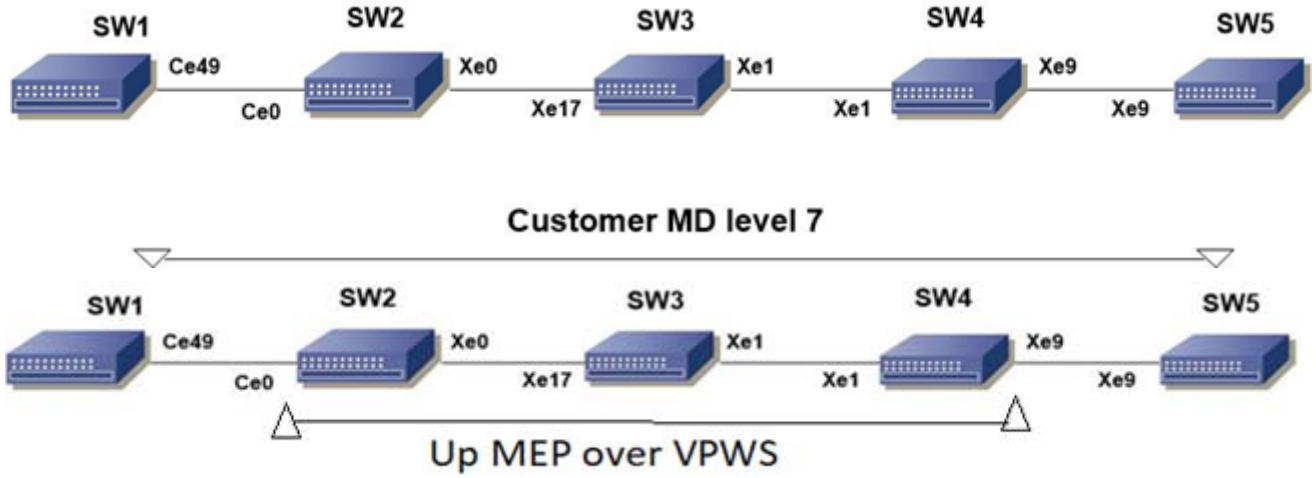


Figure 3-86: CFM Y.1731Topology

Prerequisite

Configure below hardware-profile commands related to CFM in configuration mode and reboot the nodes.

```
hardware-profile filter cfm-domain-name-str enable
hardware-profile statistics cfm-ccm enable
```

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering vlan database
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.

SW1(config-vlan)#exit	Exit vlan database
SW1(config)#int ce49	Configure interface ce49.
SW1(config-if)#switchport	Configure the interface as switch port.
SW1(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW1(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW1(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW1(config-if)#exit	Exit config mode.
SW1(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW1(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW1(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true local-vid 512 ce49	Create down mep for local-vid on ce49.
SW1(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode.
SW1(config-ether-cfm-ma)#mep crosscheck mpid 1	Configure crosscheck to remote MEP in VLAN 512.
SW1(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW1(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW1(config-ether-cfm)#exit	Exit ethernet CFM mode.

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW2(config)#vlan database	Entering vlan database
SW2(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW2(config-vlan)#exit	Exit vlan database
SW2(config)#int ce0	Configure interface ce0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce0.
SW2(config-if)#exit	Exit config mode.
SW2(config)#int xe0	Configure interface xe0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.

SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW2(config-if)#exit	Exit config mode.

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW3(config)#vlan database	Entering vlan database
SW3(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW3(config-vlan)#exit	Exit vlan database
SW3(config)#int xe17	Configure interface xe17
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe17.
SW3(config-if)#exit	Exit config mode.
SW3(config)#int xe1	Configure interface xe1.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW3(config-if)#exit	Exit config mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW4(config)#vlan database	Entering vlan database
SW4(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW4(config-vlan)#exit	Exit vlan database
SW4(config)#int xe1	Configure interface xe1.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW4(config-if)#exit	Exit config mode.
SW4(config)#int xe9	Configure interface xe9.

SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW4(config-if)#exit	Exit config mode.

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering vlan database
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit vlan database
SW5(config)#int xe9	Configure interface xe9.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW5(config-if)#exit	Exit config mode.
SW5(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW5(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW5(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true local-vid 512 xe9	Create down mep for local-vid on xe9.
SW5(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet ma-mep mode.
SW5(config-ether-cfm-ma)#mep crosscheck mpid 2	Configure crosscheck to remote MEP in VLAN 512.
SW5(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW5(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW5(config-ether-cfm)#exit	Exit ethernet CFM mode.

Validation

```
SW1#ping ethernet mac 3c2c.9926.e683 unicast source 2 domain mdnam vlan 512 bridge 1
success rate is 100 (5/5)


SW1#traceroute ethernet 3c2c.9926.e683 mepid 2 domain mdnam vlan 512 bridge 1
```

```
MP Mac Hops  Relay-action    Ingress/Egress      Ingress/Egress      action
3c2c.9926.e683    1     RlyHit     Ingress     IngOK

SW1#show ethernet cfm statistics Continuity Check Messages
CCM Sent     : 184876
CCM Received     : 21651

Loop Back Messages
LBM Sent     : 10
LBR Received(Valid)     : 10 LBR Received(Bad msdu)     : 0 LBR Received(Out-of-Seq): 0

Link Trace Messages
LTM Sent     : 1
LTR Sent     : 0
LTR Received(Valid)     : 1 LTR Received(unexpected): 0

SW1#show ethernet cfm maintenance-points local mep domain mdnam bridge 1
MPID Dir Lvl VLAN CC-Stat HW-Status     CC-Intvl MAC-Address     Def Port     MD Name
------------------------------------------------------------------------------
--
2    Dn     7     512     Enable     Installed     10 ms     6cb9.c567.721d F     ce49
mdnam

SW1#show ethernet cfm maintenance-points remote domain mdnam bridge 1 MEPID    RMEPID
LEVEL     VLAN     Rx CCM     RDI     PEER-MAC     TYPE
------------------------------------------------------------------------------
-2     1     7     512     Yes     False     3c2c.9926.e683 Configured

SW1#show ethernet cfm ma status domain mdnam vlan 512 bridge 1 MA
NAME     VLAN     STATUS
-----------------------------------------
testtm     512     Active
```

Continuity Check Message (CCM) Over VPWS

Note: The MEP should not be created on a network interface with L3 component (support is only for UpMep on VPWS).

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering VLAN database.
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit config mode.
`SW1(config)#interface ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.

SW1(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW1(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW1(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW1(config-if)#exit	Exit config mode.

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)#interface ce0	Configure interface ce0.
SW2(config-if)#switchport	Configure interface as a switch port.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface xe0	Configure interface xe0.
SW2(config-if)#no switchport	Configure interface as router port.
SW2(config-if)#ip address 10.0.0.1/24	Assign IP address to router port xe0
SW2(config-if)#no shutdown	Making the interface up
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface lo	Configure interface lo
SW2(config-if)#ip address 1.1.1.1/32 secondary	Configure secondary IP address to loopback interface .
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ospf 100	Configure ospf
SW2(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW2(config-router)#network 1.1.1.1/32 area 0	Advertising loopback IP
SW2(config-router)#exit	Exit router mode.
SW2(config)#router rsvp	Configuring rsvp
SW2(config-router)#hello-receipt	Configuring hello reception
SW2(config-router)#no-php	Configuring device as not a PHP
SW2(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW2(config-router)#exit	Exit router mode.
SW2(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW2(config-trunk)#to 2.2.2.2	Configuring first hop
SW2(config-trunk)#to 3.3.3.3	Configuring second hop
SW2(config-trunk)#exit	Exit trunk mode.
SW2(config)#interface xe0	Configuring interface
SW2(config-if)#enable-rsvp	Enabling RSVP in interface
SW2(config-if)#label-switching	Enabling MPLS labeling
SW2(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ldp	Configuring LDP
SW2(config-router)#targeted-peer ipv4 3.3.3.3	Configuring LDP target peer for PW

SW2(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW2(config-router)#no multicast-hellos	Disabling LDP multicast
SW2(config-router)#exit	Exit router mode.
SW2(config)#mpls l2-circuit ETH-2001 1 3.3.3.3	Creating VPWS PW
SW2(config)#service-template ETH-2001	Configuring service template profile for PW
SW2(config-svc)#match outer-vlan 200	Configuring match condition
SW2(config-svc)# rewrite ingress push 2000	Configuring action for match
SW2(config-svc)#exit	Exit service template mode
SW2(config)#interface ce0	Configuring interface
SW2(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW2(config-if)#exit	Exit interface mode.
SW2(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW2(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW2(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW2(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW2(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 1	Configuring remote mep
SW2(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 4001 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW2(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW2(config-ether-cfm-mpls-ma-mep)#end	Exit config mode
SW2#conf t	Config mode
SW2(config)#ethernet cfm loss-measurement profile-name lmm	Configuring LM profile
SW2(config-cfm-lm)#measurement-type lmm	Configuring measurement type as LMM
SW2(config-cfm-lm)#message-period 3	Configuring message period
SW2(config-cfm-lm)#measurement-interval 1	Configuring measurement interval
SW2(config-cfm-lm)#intervals-stored 3	Configuring number of interval to be stored
SW2(config-cfm-lm)#end	Exit config mode

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#interface xe17	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 20.0.0.1/24	Assign IP address to router port

SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe1	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 10.0.0.2/24	Assign IP address to router port
SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface lo	Configure interface lo
SW3(config-if)#ip address 2.2.2.2/32 secondary	Configure secondary IP address to loopback interface .
SW3(config-if)#exit	Exit interface mode.
SW3(config)#router ospf 100	Configure ospf
SW3(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 2.2.2.2/32 area 0	Advertising loopback IP
SW3(config-router)#exit	Exit router mode.
SW3(config)#router rsvp	Configuring rsvp
SW3(config-router)#hello-receipt	Configuring hello reception
SW3(config-router)#no-php	Configuring device as not a PHP
SW3(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW3(config-router)#exit	Exit router mode.
SW3(config)#interface xe1	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe17	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#interface xe9	Configure interface
SW4(config-if)#switchport	Configure interface as switch port.
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface xe1	Configure interface
SW4(config-if)#no switchport	Configure interface as router port.

SW4(config-if)#ip address 20.0.0.2/24	Assign IP address to router port
SW4(config-if)#no shutdown	Making the interface up
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface lo	Configure interface lo
SW4(config-if)#ip address 3.3.3.3/32 secondary	Configure secondary IP address to loopback interface .
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ospf 100	Configure ospf
SW4(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW4(config-router)#network 3.3.3.3/32 area 0	Advertising loopback IP
SW4(config-router)#exit	Exit router mode.
SW4(config)#router rsvp	Configuring rsvp
SW4(config-router)#hello-receipt	Configuring hello reception
SW4(config-router)#no-php	Configuring device as not a PHP
SW4(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW4(config-router)#exit	Exit router mode.
SW4(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW4(config-trunk)#to 2.2.2.2	Configuring first hop
SW4(config-trunk)#to 1.1.1.1	Configuring second hop
SW4(config-trunk)#exit	Exit trunk mode.
SW4(config)#interface xe1	Configuring interface
SW4(config-if)#enable-rsvp	Enabling RSVP in interface
SW4(config-if)#label-switching	Enabling MPLS labeling
SW4(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ldp	Configuring LDP
SW4(config-router)#targeted-peer ipv4 1.1.1.1	Configuring LDP target peer for PW
SW4(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW4(config-router)#no multicast-hellos	Disabling LDP multicast
SW4(config-router)#exit	Exit router mode.
SW4(config)#mpls l2-circuit ETH-2001 1 1.1.1.1	Creating VPWS PW
SW4(config)#service-template ETH-2001	Configuring service template profile for PW
SW4(config-svc)# match outer-vlan 200	Configuring match condition
SW4(config-svc)# rewrite ingress push 2000	Configuring action for match
SW4(config-svc)#exit	Exit service template mode
SW4(config)#interface xe9	Configuring interface
SW4(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW4(config-if)#exit	Exit interface mode.

SW4(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW4(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW4(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW4(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW4(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 4001	Configuring remote mep
SW4(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 1 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW4(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW4(config-ether-cfm-mpls-ma-mep)#ethernet cfm loss-measurement reply lmm	Configuring LMR
SW4(config-ether-cfm-mpls-ma-mep)#end	Exit config mode

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering VLAN database.
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit config mode.
SW5(config)#interface xe9	Configure interface ce49.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW5(config-if)#exit	Exit config mode.

Validation

```
SW1#show ethernet cfm maintenance-points remote domain 12345 vpws
 MEPID     RMEPID     LEVEL     Rx CCM    RDI    PEER-MAC        TYPE
------------------------------------------------------------------------
 200       100        7         Yes       False  b86a.97d2.27d0 Configured

SW1#show ethernet cfm ma status domain 12345 vpws
MA NAME                  STATUS
-------------------------------
  43981                  Active
```

CHAPTER 4 Y.1731 Performance Monitoring Configurations

ITU-T Y.1731 supports Performance Monitoring feature for Ethernet. Loss and Delay measurement can be achieved which can be significantly used to identify network problems before they impact. SLM is used to calculate the frame loss between endpoints using synthetic frames. Transmit and received counters at endpoints for received vs dropped are used to measure frame loss. CCM and LMM are used to calculate the frame loss of data traffic between endpoints. On CCM, loss measurement is encapsulated as part of CFM packets and it's dual ended. For LMM, separate loss measurement message and reply is shared on configured interval between endpoints to calculate the data frame loss. CCM and LMM service frames will have the counters which maintain a count of transmitted and received data frames between a pair of MEPs.Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor SLAs. Ethernet frame delay measure-ment also collects other useful information, such as worst and best case delays, average delay, and aver-age delay variation.

Synthetic Loss Measurement (SLM)

Topology

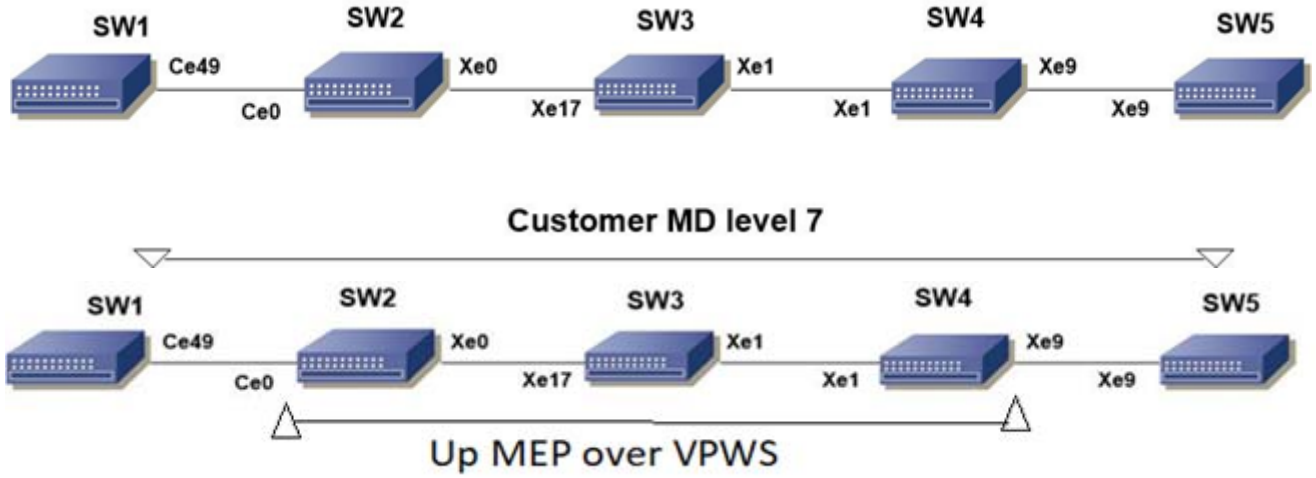


Figure 4-87: CFM Y.1731Topology

Prerequisite

Configure below hardware-profile commands related to CFM in configuration mode and reboot the nodes.

```
hardware-profile filter cfm-domain-name-str enable
hardware-profile statistics cfm-ccm enable
```

Synthetic Loss Measurement (SLM)

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering VLAN database.
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit config mode.
`SW1(config)#int ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.
`SW1(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1`	Create cfm domain with type as character string and set mip creation criteria to default.
`SW1(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default`	Create ma type as string and set mip creation criteria to default.
`SW1(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true local-vid 512 ce49`	Create down mep for local-vid on ce49.
`SW1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast.
`SW1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode.
`SW1(config-ether-cfm-ma)#mep crosscheck mpid 1`	Configure crosscheck to remote MEP in VLAN 512.
`SW1(config-ether-cfm-ma)#cc interval 2`	Enable cc interval for 10 millisecond.
`SW1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit ethernet ma mode.
`SW1(config-ether-cfm)#exit`	Exit ethernet CFM mode.
`SW1(config)#ethernet cfm loss-measurement profile-name SLM`	Creating loss-measurement profile for SLM
`SW1(config-cfm-lm)#measurement-interval 1`	Specify the measurement-interval in minutes
`SW1(config)#intervals-stored 3`	Specify the number of history interval to be stored
`SW1(config)# message-period 1`	Specify message period interval time

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW2(config)#vlan database`	Entering VLAN database.

SW2(config-vlan)#vlan 512 type customer bridge 1 state enable	Create VLAN 512 for customer bridge.
SW2(config-vlan)#exit	Exit config mode.
SW2(config)#int ce0	Configure interface ce0.
SW2(config-if)#switchport	Configure interface as a switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all customer VLANs on interface ce0.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#int xe0	Configure interface xe0
SW2(config-if)#switchport	Configure interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1
SW2(config-if)#exit	Exit config mode.

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW3(config)#vlan database	Entering VLAN database.
SW3(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW3(config-vlan)#exit	Exit config mode.
SW3(config)#int xe17	Configure interface xe17.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe17.
SW3(config-if)#exit	Exit config mode.
SW3(config)#int xe1	Configure interface xe1.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW3(config-if)#exit	Exit config mode.

SW4

`SW4#configure terminal`	Enter configure mode.
`SW4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW4(config)#vlan database`	Entering VLAN database.
`SW4(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW4(config-vlan)#exit`	Exit config mode.
`SW4(config)#int xe1`	Configure interface xe1.
`SW4(config-if)#switchport`	Configure the interface as switch port.
`SW4(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW4(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW4(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface xe1.
`SW4(config-if)#exit`	Exit config mode.
`SW4(config)#int xe9`	Configure interface xe9.
`SW4(config-if)#switchport`	Configure the interface as switch port.
`SW4(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW4(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW4(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface xe9.
`SW4(config-if)#exit`	Exit config mode.

SW5

`SW5#configure terminal`	Enter configure mode.
`SW5(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW5(config)#vlan database`	Entering VLAN database.
`SW5(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW5(config-vlan)#exit`	Exit config mode.
`SW5(config)#int xe9`	Configure interface xe9.
`SW5(config-if)#switchport`	Configure the interface as switch port.
`SW5(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW5(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW5(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface xe9.
`SW5(config-if)#exit`	Exit config mode.
`SW5(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1`	Create cfm domain with type as character string and set mip creation criteria to default.
`SW5(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default`	Create ma type as string and set mip creation criteria to default.

SW5(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true local-vid 512 xe9	Create down mep for local-vid on xe9
SW5(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW5(config-ether-cfm-ma-mep)#ethernet cfm loss-measurement reply slm	Generate and send SLR responses tacked
SW5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode.
SW5(config-ether-cfm-ma)#mep crosscheck mpid 2	Configure crosscheck to remote MEP in VLAN 512.
SW5(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW5(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW5(config-ether-cfm)#exit	Exit ethernet CFM mode.

Commands to initiate/abort loss measurement

```
SW1#loss-measurement type proactive profile-name <WORD> rmep mac-address
<HHHH.HHHH.HHHH>mep <MEPID> domain < DOMAIN_NAME> vlan <VLANID>bridge <1-32>

SW1#abort loss-measurement mep <MEPID> domain <DOMAIN_NAME> vlan <VLANID> bridge <1-32>
```

Validation

```
SW1#ping ethernet mac 3c2c.9926.e683 unicast source 2 domain mdnam vlan 512 bridge 1
success rate is     100 (5/5)


SW1#traceroute ethernet 3c2c.9926.e683 mepid 2 domain mdnam vlan 512 bridge 1 MP Mac
Hops     Relay-action     Ingress/Egress     Ingress/Egress ac-tion
3c2c.9926.e683     1     RlyHit     Ingress     IngOK

SW1#loss-measurement type proactive profile-name SLM rmep mac-address 3c2c.9926.e683
mep 2 domain mdnam vlan 512 bridge 1


SW1#show ethernet cfm loss-measurement mep 2 domain mdnam vlan 512 bridge 1
MEP: 2 MA: testtm
CURRENT:
Measurement ID             :1
Suspect                    :True
Measurement Type           :slm
Elapsed time(sec)          :7
Start Time                 :2019 Apr 30 14:43:41
Near End loss              :0
Far End loss               :0
Near End accumulated loss  : 0
Far End accumulated loss   : 0
SW1# abort loss-measurement mep 2 domain mdnam vlan 512 bridge 1
```

Synthetic Loss Measurement (SLM) Over VPWS

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering VLAN database.
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit config mode.
`SW1(config)#interface ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#interface ce0`	Configure interface ce0.
`SW2(config-if)#switchport`	Configure interface as a switch port.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface xe0`	Configure interface xe1.
`SW2(config-if)#no switchport`	Configure interface as router port.
`SW2(config-if)#ip address 10.0.0.1/24`	Assign IP address to router port xe0
`SW2(config-if)#no shutdown`	Making the interface up
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface lo`	Configure interface lo
`SW2(config-if)#ip address 1.1.1.1/32 secondary`	Configure secondary IP address to loopback interface .
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#router ospf 100`	Configure ospf
`SW2(config-router)#network 10.0.0.0/24 area 0`	Advertising 10 network
`SW2(config-router)#network 1.1.1.1/32 area 0`	Advertising loopback IP
`SW2(config-router)#exit`	Exit router mode.
`SW2(config)#router rsvp`	Configuring rsvp
`SW2(config-router)#hello-receipt`	Configuring hello reception
`SW2(config-router)#no-php`	Configuring device as not a PHP
`SW2(config-router)#revert-timer 10`	Configuring reversion time of RSVP

SW2(config-router)#exit	Exit router mode.
SW2(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW2(config-trunk)#to 2.2.2.2	Configuring first hop
SW2(config-trunk)#to 3.3.3.3	Configuring second hop
SW2(config-trunk)#exit	Exit trunk mode.
SW2(config)#interface xe0	Configuring interface
SW2(config-if)#enable-rsvp	Enabling RSVP in interface
SW2(config-if)#label-switching	Enabling MPLS labeling
SW2(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ldp	Configuring LDP
SW2(config-router)#targeted-peer ipv4 3.3.3.3	Configuring LDP target peer for PW
SW2(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW2(config-router)#no multicast-hellos	Disabling LDP multicast
SW2(config-router)#exit	Exit router mode.
SW2(config)#mpls l2-circuit ETH-2001 1 3.3.3.3	Creating VPWS PW
SW2(config)#service-template ETH-2001	Configuring service template profile for PW
SW2(config-svc)#match outer-vlan 10	Configuring match condition
SW2(config-svc)# rewrite ingress push 2000	Configuring action for match
SW2(config-svc)#exit	Exit service template mode
SW2(config)#interface ce0	Configuring interface
SW2(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW2(config-if)#exit	Exit interface mode.
SW2(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW2(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW2(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW2(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW2(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 1	Configuring remote mep
SW2(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 4001 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW2(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW2(config-ether-cfm-mpls-ma-mep)#end	Exit config mode
SW2#conf t	Config mode

SW2(config)#ethernet cfm loss-measurement profile-name slm	Configuring LM profile
SW2(config-cfm-lm)#measurement-type slm	Configuring measurement type as SLM
SW2(config-cfm-lm)#message-period 3	Configuring message period
SW2(config-cfm-lm)#measurement-interval 1	Configuring measurement interval
SW2(config-cfm-lm)#intervals-stored 3	Configuring number of interval to be stored
SW2(config-cfm-lm)#end	Exit config mode

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#interface xe17	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 20.0.0.1/24	Assign IP address to router port
SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe1	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 10.0.0.2/24	Assign IP address to router port
SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface lo	Configure interface lo
SW3(config-if)#ip address 2.2.2.2/32 secondary	Configure secondary IP address to loopback interface .
SW3(config-if)#exit	Exit interface mode.
SW3(config)#router ospf 100	Configure ospf
SW3(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 2.2.2.2/32 area 0	Advertising loopback IP
SW3(config-router)#exit	Exit router mode.
SW3(config)#router rsvp	Configuring rsvp
SW3(config-router)#hello-receipt	Configuring hello reception
SW3(config-router)#no-php	Configuring device as not a PHP
SW3(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW3(config-router)#exit	Exit router mode.
SW3(config)#interface xe1	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe17	Configuring interface

SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#interface xe9	Configure interface
SW4(config-if)#switchport	Configure interface as switch port.
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface xe1	Configure interface
SW4(config-if)#no switchport	Configure interface as router port.
SW4(config-if)#ip address 20.0.0.2/24	Assign IP address to router port
SW4(config-if)#no shutdown	Making the interface up
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface lo	Configure interface lo
SW4(config-if)#ip address 3.3.3.3/32 secondary	Configure secondary IP address to loopback interface .
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ospf 100	Configure ospf
SW4(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW4(config-router)#network 3.3.3.3/32 area 0	Advertising loopback IP
SW4(config-router)#exit	Exit router mode.
SW4(config)#router rsvp	Configuring rsvp
SW4(config-router)#hello-receipt	Configuring hello reception
SW4(config-router)#no-php	Configuring device as not a PHP
SW4(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW4(config-router)#exit	Exit router mode.
SW4(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW4(config-trunk)#to 2.2.2.2	Configuring first hop
SW4(config-trunk)#to 1.1.1.1	Configuring second hop
SW4(config-trunk)#exit	Exit trunk mode.
SW4(config)#interface xe1	Configuring interface
SW4(config-if)#enable-rsvp	Enabling RSVP in interface
SW4(config-if)#label-switching	Enabling MPLS labeling
SW4(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ldp	Configuring LDP
SW4(config-router)#targeted-peer ipv4 1.1.1.1	Configuring LDP target peer for PW

SW4(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW4(config-router)#no multicast-hellos	Disabling LDP multicast
SW4(config-router)#exit	Exit router mode.
SW4(config)#mpls l2-circuit ETH-2001 1 1.1.1.1	Creating VPWS PW
SW4(config)#service-template ETH-2001	Configuring service template profile for PW
SW4(config-svc)# match outer-vlan 200	Configuring match condition
SW4(config-svc)# rewrite ingress push 2000	Configuring action for match
SW4(config-svc)#exit	Exit service template mode
SW4(config)#interface xe9	Configuring interface
SW4(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW4(config-if)#exit	Exit interface mode.
SW4(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW4(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW4(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW4(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW4(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 4001	Configuring remote mep
SW4(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 1 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW4(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW4(config-ether-cfm-mpls-ma-mep)#ethernet cfm loss-measurement reply slm	Configuring SLR
SW4(config-ether-cfm-mpls-ma-mep)#end	Exit config mode

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering VLAN database.
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit config mode.
SW5(config)#interface xe9	Configure interface ce49.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.

SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW5(config-if)#exit	Exit config mode.

Commands to initiate/abort loss measurement

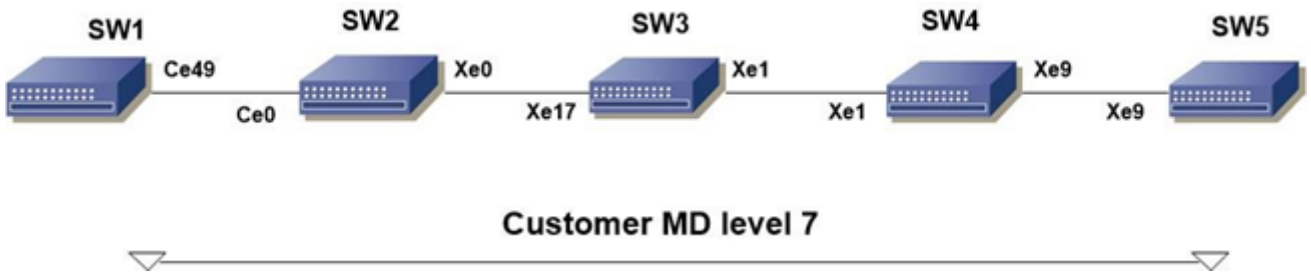
```
SW2#loss-measurement type proactive profile-name <WORD> rmep mac-address
<HHHH.HHHH.HHHH>mep <MEPID> domain < DOMAIN_NAME> vpws <VCNAME>

SW2#abort loss-measurement mep <MEPID> domain <DOMAIN_NAME> vpws <VCNAME>
```

Validation

```
SW2#loss-measurement type proactive profile-name slm rmep mac-address 3c2c.9926.e683
mep 1 domain 12345 vpws ETH-2001

SW2#show ethernet cfm loss-measurement mep 1 domain 12345 vpws ETH-2001
MEP: 2 MA: 43981
CURRENT:
Measurement ID             : 1
Suspect                    : False
Measurement Type           : slm
Elapsed time(sec)          : 7
Start Time                 : 2019 Apr 30 14:43:41
Near End loss              : 0
Far End loss               : 0
Near End accumulated loss  : 0
Far End accumulated loss   : 0

SW2# abort loss-measurement mep 1 domain 12345 vpws ETH-2001
```

Loss Measurement Message(LMM)

Topology



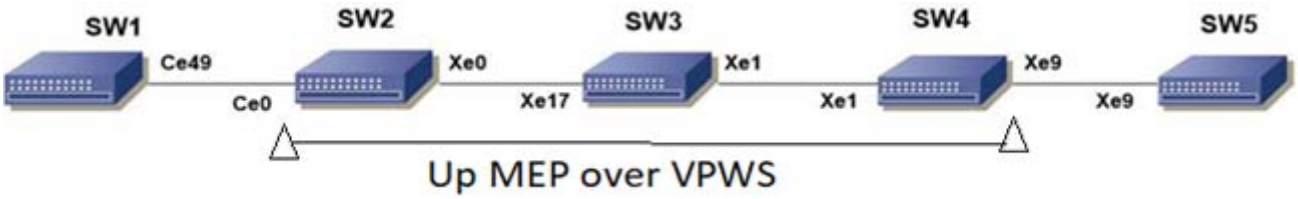


Figure 4-88: CFM Y.1731Topology

Prerequisite

Configure below hardware-profile commands related to CFM in configuration mode and reboot the nodes.

```
hardware-profile filter cfm-domain-name-str enable
hardware-profile statistics cfm-lm enable
hardware-profile statistics cfm-ccm enable
```

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering vlan database
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit vlan database
`SW1(config)#int ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.
`SW1(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1`	Create cfm domain with type as character string and set mip creation criteria to default.
`SW1(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default`	Create ma type as string and set mip creation criteria to default.
`SW1(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true local-vid 512 ce49`	Create down mep for local-vid on ce49.
`SW1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast.
`SW1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode.
`SW1(config-ether-cfm-ma)#mep crosscheck mpid 1`	Configure crosscheck to remote MEP in VLAN 512.
`SW1(config-ether-cfm-ma)#cc interval 2`	Enable cc interval for 10 millisecond.
`SW1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit ethernet ma mode.
`SW1(config-ether-cfm)#exit`	Exit ethernet CFM mode.

SW1(config)# ethernet cfm loss-measurement profile-name LMM	Creating loss-measurement profile for LMM
SW1(config-cfm-lm)# measurement-type lmm	Specify the measurement type
SW1(config-cfm-lm)# measurement-interval 1	Specify the measurement-interval in minutes
SW1(config)# intervals-stored 3	Specify the number of history interval to be stored
SW1(config)# message-period 1	Specify message period interval time

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW2(config)#vlan database	Entering vlan database
SW2(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW2(config-vlan)#exit	Exit vlan database
SW2(config)#int ce0	Configure interface ce0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce0.
SW2(config-if)#exit	Exit config mode.
SW2(config)#int xe0	Configure interface xe0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW2(config-if)#exit	Exit config mode.

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW3(config)#vlan database	Entering vlan database
SW3(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW3(config-vlan)#exit	Exit vlan database
SW3(config)#int xe17	Configure interface xe17.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.

SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe17.
SW3(config-if)#exit	Exit config mode.
SW3(config)#int xe1	Configure interface xe1.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW3(config-if)#exit	Exit config mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW4(config)#vlan database	Entering vlan database
SW4(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW4(config-vlan)#exit	Exit vlan database
SW4(config)#int xe1	Configure interface xe1.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW4(config-if)#exit	Exit config mode.
SW4(config)#int xe9	Configure interface xe9.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW4(config-if)#exit	Exit config mode.

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering vlan database
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit vlan database
SW5(config)#int xe9	Configure interface xe9.

SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW5(config-if)#exit	Exit config mode.
SW5(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW5(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW5(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true local-vid 512 xe9	Create down mep for local-vid on xe9
SW5(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW5(config-ether-cfm-ma-mep)#ethernet cfm loss-measurement reply lmm	Generate and send LMR responses tacked
SW5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode.
SW5(config-ether-cfm-ma)#mep crosscheck mpid 2	Configure crosscheck to remote MEP in VLAN 512.
SW5(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW5(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW5(config-ether-cfm)#exit	Exit ethernet CFM mode.

Commands to initiate/abort loss measurement

```
loss-measurement type on-demand profile-name <WORD> rmep mac-address <HHHH.HHHH.HHHH> start-time <immediate|relative|absolute> stop-time <none|absolute|relative> repetition-period <REP-TIME> mep <MEPID> domain < DOMAIN_NAME> vlan <VLANID>bridge <1-32>


loss-measurement type proactive profile-name <WORD> rmep mac-address <HHHH.HHHH.HHHH>mep <MEPID> domain < DOMAIN_NAME> vlan <VLANID>bridge <1-32>


abort loss-measurement mep <MEPID> domain <DOMAIN_NAME> vlan <VLANID> bridge <1-32>


clear loss-measurement mep <MEPID> domain <DOMAIN_NAME> vlan <VLANID> bridge <1-32>
```

Validation

```
SW1#ping ethernet mac 3c2c.9926.e683 unicast source 2 domain mdnam vlan 512 bridge 1
 success rate is  100 (5/5)


SW1#traceroute ethernet 3c2c.9926.e683 mepid 2 domain mdnam vlan 512 bridge 1
 MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress action
3c2c.9926.e683   1     RlyHit                Ingress         IngOK


SW1# loss-measurement type proactive profile-name LMM rmep mac-address 3c2c.9926.e683 mep 2 domain mdnam vlan 512 bridge 1
```

```
SW1# show ethernet cfm loss-measurement mep 2 domain mdnam vlan 512 bridge 1
MEP: 2 MA: testtm
CURRENT:
 Measurement ID              : 1
  Suspect                    : False
  Measurement Type           : lmm
  Elapsed time(sec)          : 24
  Start Time                 : 2019 Jul 21 00:10:36
  Near End loss              : 0
  Far End loss               : 0
  Near End accumulated loss  : 0
  Far End accumulated loss   : 0

SW1# abort loss-measurement mep 2 domain mdnam vlan 512 bridge 1
```

Loss Measurement Message (LMM) Over VPWS

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering VLAN database.
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit config mode.
`SW1(config)#interface ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#interface ce0`	Configure interface ce0.
`SW2(config-if)#switchport`	Configure interface as a switch port.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface xe0`	Configure interface xe0.
`SW2(config-if)#no switchport`	Configure interface as router port.
`SW2(config-if)#ip address 10.0.0.1/24`	Assign IP address to router port xe0
`SW2(config-if)#no shutdown`	Making the interface up
`SW2(config-if)#exit`	Exit interface mode.

SW2(config)#interface lo	Configure interface lo
SW2(config-if)#ip address 1.1.1.1/32 secondary	Configure secondary IP address to loopback interface .
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ospf 100	Configure ospf
SW2(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW2(config-router)#network 1.1.1.1/32 area 0	Advertising loopback IP
SW2(config-router)#exit	Exit router mode.
SW2(config)#router rsvp	Configuring rsvp
SW2(config-router)#hello-receipt	Configuring hello reception
SW2(config-router)#no-php	Configuring device as not a PHP
SW2(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW2(config-router)#exit	Exit router mode.
SW2(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW2(config-trunk)#to 2.2.2.2	Configuring first hop
SW2(config-trunk)#to 3.3.3.3	Configuring second hop
SW2(config-trunk)#exit	Exit trunk mode.
SW2(config)#interface xe0	Configuring interface
SW2(config-if)#enable-rsvp	Enabling RSVP in interface
SW2(config-if)#label-switching	Enabling MPLS labeling
SW2(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ldp	Configuring LDP
SW2(config-router)#targeted-peer ipv4 3.3.3.3	Configuring LDP target peer for PW
SW2(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW2(config-router)#no multicast-hellos	Disabling LDP multicast
SW2(config-router)#exit	Exit router mode.
SW2(config)#mpls l2-circuit ETH-2001 1 3.3.3.3	Creating VPWS PW
SW2(config)#service-template ETH-2001	Configuring service template profile for PW
SW2(config-svc)#match outer-vlan 200	Configuring match condition
SW2(config-svc)# rewrite ingress push 2000	Configuring action for match
SW2(config-svc)#exit	Exit service template mode
SW2(config)#interface ce0	Configuring interface
SW2(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW2(config-if)#exit	Exit interface mode.
SW2(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name

SW2(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW2(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW2(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW2(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 1	Configuring remote mep
SW2(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 4001 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW2(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW2(config-ether-cfm-mpls-ma-mep)#end	Exit config mode
SW2#conf t	Config mode
SW2(config)#ethernet cfm loss-measurement profile-name lmm	Configuring LM profile
SW2(config-cfm-lm)#measurement-type lmm	Configuring measurement type as LMM
SW2(config-cfm-lm)#message-period 3	Configuring message period
SW2(config-cfm-lm)#measurement-interval 1	Configuring measurement interval
SW2(config-cfm-lm)#intervals-stored 3	Configuring number of interval to be stored
SW2(config-cfm-lm)#end	Exit config mode

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#interface xe17	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 20.0.0.1/24	Assign IP address to router port
SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe1	Configure interface
SW3(config-if)#no switchport	Configure interface as router port.
SW3(config-if)#ip address 10.0.0.2/24	Assign IP address to router port
SW3(config-if)#no shutdown	Making the interface up
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface lo	Configure interface lo
SW3(config-if)#ip address 2.2.2.2/32 secondary	Configure secondary IP address to loopback interface.
SW3(config-if)#exit	Exit interface mode.
SW3(config)#router ospf 100	Configure ospf
SW3(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network

SW3(config-router)#network 2.2.2.2/32 area 0	Advertising loopback IP
SW3(config-router)#exit	Exit router mode.
SW3(config)#router rsvp	Configuring rsvp
SW3(config-router)#hello-receipt	Configuring hello reception
SW3(config-router)#no-php	Configuring device as not a PHP
SW3(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW3(config-router)#exit	Exit router mode.
SW3(config)#interface xe1	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe17	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#interface xe9	Configure interface
SW4(config-if)#switchport	Configure interface as switch port.
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface xe1	Configure interface
SW4(config-if)#no switchport	Configure interface as router port.
SW4(config-if)#ip address 20.0.0.2/24	Assign IP address to router port
SW4(config-if)#no shutdown	Making the interface up
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface lo	Configure interface lo
SW4(config-if)#ip address 3.3.3.3/32 secondary	Configure secondary IP address to loopback interface .
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ospf 100	Configure ospf
SW4(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW4(config-router)#network 3.3.3.3/32 area 0	Advertising loopback IP
SW4(config-router)#exit	Exit router mode.
SW4(config)#router rsvp	Configuring rsvp
SW4(config-router)#hello-receipt	Configuring hello reception
SW4(config-router)#no-php	Configuring device as not a PHP
SW4(config-router)#revert-timer 10	Configuring reversion time of RSVP

SW4(config-router)#exit	Exit router mode.
SW4(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW4(config-trunk)#to 2.2.2.2	Configuring first hop
SW4(config-trunk)#to 1.1.1.1	Configuring second hop
SW4(config-trunk)#exit	Exit trunk mode.
SW4(config)#interface xe1	Configuring interface
SW4(config-if)#enable-rsvp	Enabling RSVP in interface
SW4(config-if)#label-switching	Enabling MPLS labeling
SW4(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ldp	Configuring LDP
SW4(config-router)#targeted-peer ipv4 1.1.1.1	Configuring LDP target peer for PW
SW4(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW4(config-router)#no multicast-hellos	Disabling LDP multicast
SW4(config-router)#exit	Exit router mode.
SW4(config)#mpls l2-circuit ETH-2001 1 1.1.1.1	Creating VPWS PW
SW4(config)#service-template ETH-2001	Configuring service template profile for PW
SW4(config-svc)# match outer-vlan 200	Configuring match condition
SW4(config-svc)# rewrite ingress push 2000	Configuring action for match
SW4(config-svc)#exit	Exit service template mode
SW4(config)#interface xe9	Configuring interface
SW4(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW4(config-if)#exit	Exit interface mode.
SW4(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW4(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW4(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW4(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW4(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 4001	Configuring remote mep
SW4(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 1 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service
SW4(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW4(config-ether-cfm-mpls-ma-mep)#ethernet cfm loss-measurement reply lmm	Configuring LMR
SW4(config-ether-cfm-mpls-ma-mep)#end	Exit config mode

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering VLAN database.
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit config mode.
SW5(config)#interface xe9	Configure interface ce49.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW5(config-if)#exit	Exit config mode.

Commands to initiate/abort loss measurement

```
SW2#loss-measurement type proactive profile-name <WORD> rmep mac-address
<HHHH.HHHH.HHHH>mep <MEPID> domain < DOMAIN_NAME> vpws <VCNAME>

SW2#abort loss-measurement mep <MEPID> domain <DOMAIN_NAME> vpws <VCNAME>
```

Validation

```
SW2#loss-measurement type proactive profile-name lmm rmep mac-address 3c2c.9926.e683
mep 1 domain 12345 vpws ETH-2001

SW2#show ethernet cfm loss-measurement mep 1 domain 12345 vpws ETH-2001
MEP: 2 MA: 43981
CURRENT:
Measurement ID               : 1
Suspect                      : False
Measurement Type             : lmm
Elapsed time(sec)            : 7
Start Time                   : 2019 Apr 30 14:43:41
Near End loss                : 0
Far End loss                 : 0
Near End accumulatedloss     : 0
Far End accumulated loss     : 0
SW2# abort loss-measurement mep 1 domain 12345 vpws ETH-2001
```

Delay Measurement(DM)

Topology

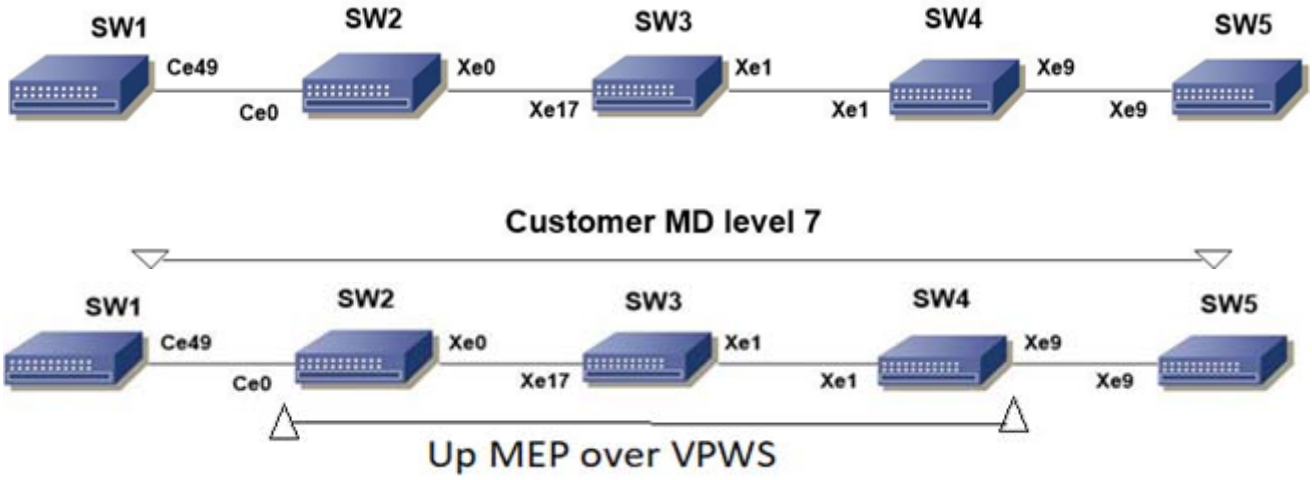


Figure 4-89: CFM Y.1731Topology

Prerequisite

Configure below hardware-profile commands related to CFM in configuration mode and reboot the nodes.

```
hardware-profile filter cfm-domain-name-str enable
hardware-profile statistics ingress-acl enable
hardware-profile statistics cfm-lm enable
hardware-profile statistics cfm-ccm enable
```

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering vlan database
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit vlan database
`SW1(config)#int ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.

SW1(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW1(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW1(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true local-vid 512 ce49	Create down mep for local-vid on ce49.
SW1(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode.
SW1(config-ether-cfm-ma)#mep crosscheck mpid 1	Configure crosscheck to remote MEP in VLAN 512.
SW1(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW1(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW1(config-ether-cfm)#exit	Exit ethernet CFM mode.
SW1(config)# ethernet cfm delay-measurement profile-name DM	Creating loss-measurement profile for DM
SW1(config-cfm-dm)# measurement-interval 1	Specify the measurement-interval in minutes
SW1(config-cfm-dm)# number-intervals-stored 3	Specify the number of history interval to be stored
SW1(config-cfm-dm)# message-period 1s	Specify message period interval time
SW1(config-cfm-dm)# bins-per-fd-interval 4	Specify the number of measurement bins per Measurement Interval for Frame Delay measurements.
SW1(config-cfm-dm)# bins-per-ifdv-interval 3	Specify the number of measurement bins per Measurement Interval for Inter-Frame Delay Variation measurements.

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW2(config)#vlan database	Entering vlan database
SW2(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW2(config-vlan)#exit	Exit vlan database
SW2(config)#int ce0	Configure interface ce0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce0.
SW2(config-if)#exit	Exit config mode.
SW2(config)#int xe0	Configure interface xe0.
SW2(config-if)#switchport	Configure the interface as switch port.
SW2(config-if)#bridge-group 1	Configure interface in bridge group 1.

SW2(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW2(config-if)#exit	Exit config mode.

SW3

SW3#configure terminal	Enter configure mode.
SW3(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW3(config)#vlan database	Entering vlan database
SW3(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW3(config-vlan)#exit	Exit vlan database
SW3(config)#int xe17	Configure interface xe17.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe17.
SW3(config-if)#exit	Exit config mode.
SW3(config)#int xe1	Configure interface xe1.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW3(config-if)#exit	Exit config mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW4(config)#vlan database	Entering vlan database
SW4(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW4(config-vlan)#exit	Exit vlan database
SW4(config)#int xe1	Configure interface xe1.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW4(config-if)#exit	Exit config mode.

SW4(config)#int xe9	Configure interface xe9.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW4(config-if)#exit	Exit config mode.

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering vlan database
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit vlan database
SW5(config)#int xe9	Configure interface xe9.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1.
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW5(config-if)#exit	Exit config mode.
SW5(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW5(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW5(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true local-vid 512 xe9	Create down mep for local-vid on xe9
SW5(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW5(config-ether-cfm-ma-mep)# ethernet cfm delay-measurement reply dmm	Generate and send DMM responses tacked
SW5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet cfm ma-mep mode.
SW5(config-ether-cfm-ma)#mep crosscheck mpid 2	Configure crosscheck to remote MEP in VLAN 512.
SW5(config-ether-cfm-ma)#cc interval 2	Enable cc interval for 10 millisecond.
SW5(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW5(config-ether-cfm)#exit	Exit ethernet CFM mode.

Commands to initiate/abort on-demand delay measurement

```
delay-measurement type on-demand profile-name WORD rmep (mac-address MAC|RMEPID) start-time (immediate|relative HH:MM:SS|absolute HH:MM:SS <1-31> MONTH <1993-2035>)
```

```
repetition-period <6000-4294967295> mep MEPID domain DOMAIN_NAME (vlan <2-4094>|)
bridge <1-32>

abort delay-measurement mep <MEPID> domain <DOMAIN_NAME> vlan <VLANID> bridge <1-32>
```

Validation

```
SW1#ping ethernet mac 3c2c.9926.e683 unicast source 2 domain mdnam vlan 512 bridge 1
 success rate is  100 (5/5)

SW1#traceroute ethernet 3c2c.9926.e683 mepid 2 domain mdnam vlan 512 bridge 1
 MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress action
3c2c.9926.e683   1     RlyHit                Ingress         IngOK

SW1# delay-measurement type proactive profile-name DM rmep mac-address 3c2c.9926.e683
mep 2 domain mdnam vlan 512 bridge 1

SW1#show ethernet cfm delay-measurement mep 2 domain mdnam vlan 512 bridge 1
 MEP                    : 2
 MA                     : testtm
 VLAN ID                : 512
 Peer MAC Address       : 3c2c.9926.e683

CURRENT:
======================
 RMEP ID                     : 1
 Measurement ID              : 12
 Measurement Type            : DMM
 Elapsed time(sec)           : 24
 Start Time                  : 2019 Aug 06 13:23:53
 Suspect Flag                : FALSE
 Min Frame Delay(usec)       : 13
 Max Frame Delay(usec)       : 13
 Avg Frame Delay(usec)       : 13
 Min Inter FD Variation(usec): 0
 Max Inter FD Variation(usec): 0
 Avg Inter FD Variation(usec): 0

             FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    3
 2             5000    - <    9999    0
 3             10000   - <   14999    0
 4             15000   - <     Inf    0

           INTER-FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    2
 2             5000    - <    9999    0
```

```
 3             10000   - <     Inf    0


HISTORY STATISTICS
======================
 MD                          : mdnam
 MA                          : testtm
 MEP                         : 2
 VLAN ID                     : 512
 RMEP ID                     : 1
 Measurement ID              : 10
 Measurement Type            : DMM
 Elapsed time(sec)           : 60
 End Time                    : 2019 Aug 06 13:22:52
 Suspect Flag                : FALSE
 Min Frame Delay(usec)       : 13
 Max Frame Delay(usec)       : 13
 Avg Frame Delay(usec)       : 13
 Min Inter FD Variation(usec): 0
 Max Inter FD Variation(usec): 0
 Avg Inter FD Variation(usec): 0

             FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    6
 2             5000    - <    9999    0
 3             10000   - <   14999    0
 4             15000   - <     Inf    0

           INTER-FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    5
 2             5000    - <    9999    0
 3             10000   - <     Inf    0

 RMEP ID        : 1
 Measurement ID : 11
 Measurement Type            : DMM
 Elapsed time(sec)           : 60
 End Time                    : 2019 Aug 06 13:23:52
 Suspect Flag                : FALSE
 Min Frame Delay(usec)       : 13
 Max Frame Delay(usec)       : 13
 Avg Frame Delay(usec)       : 13
 Min Inter FD Variation(usec): 0
 Max Inter FD Variation(usec): 0
 Avg Inter FD Variation(usec): 0
```

```
             FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    6
 2             5000    - <    9999    0
 3             10000   - <   14999    0
 4             15000   - <     Inf    0

           INTER-FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    5
 2             5000    - <    9999    0
 3             10000   - <     Inf    0

SW1# abort delay-measurement mep 2 domain mdnam vlan 512 bridge 1
```

Delay Measurement Message (LMM) Over VPWS

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering VLAN database.
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit config mode.
`SW1(config)#interface ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1`	Configure interface in bridge group 1.
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#interface ce0`	Configure interface ce0.
`SW2(config-if)#switchport`	Configure interface as a switch port.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface xe0`	Configure interface xe0.
`SW2(config-if)#no switchport`	Configure interface as router port.
`SW2(config-if)#ip address 10.0.0.1/24`	Assign IP address to router port xe0
`SW2(config-if)#no shutdown`	Making the interface up

SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface lo	Configure interface lo
SW2(config-if)#ip address 1.1.1.1/32 secondary	Configure secondary IP address to loopback interface.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ospf 100	Configure ospf
SW2(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW2(config-router)#network 1.1.1.1/32 area 0	Advertising loopback IP
SW2(config-router)#exit	Exit router mode.
SW2(config)#router rsvp	Configuring rsvp
SW2(config-router)#hello-receipt	Configuring hello reception
SW2(config-router)#no-php	Configuring device as not a PHP
SW2(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW2(config-router)#exit	Exit router mode.
SW2(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW2(config-trunk)#to 2.2.2.2	Configuring first hop
SW2(config-trunk)#to 3.3.3.3	Configuring second hop
SW2(config-trunk)#exit	Exit trunk mode.
SW2(config)#interface xe0	Configuring interface
SW2(config-if)#enable-rsvp	Enabling RSVP in interface
SW2(config-if)#label-switching	Enabling MPLS labeling
SW2(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW2(config-if)#exit	Exit interface mode.
SW2(config)#router ldp	Configuring LDP
SW2(config-router)#targeted-peer ipv4 3.3.3.3	Configuring LDP target peer for PW
SW2(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW2(config-router)#no multicast-hellos	Disabling LDP multicast
SW2(config-router)#exit	Exit router mode.
SW2(config)#mpls l2-circuit ETH-2001 1 3.3.3.3	Creating VPWS PW
SW2(config)#service-template ETH-2001	Configuring service template profile for PW
SW2(config-svc)#match outer-vlan 200	Configuring match condition
SW2(config-svc)# rewrite ingress push 2000	Configuring action for match
SW2(config-svc)#exit	Exit service template mode
SW2(config)#interface ce0	Configuring interface
SW2(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW2(config-if)#exit	Exit interface mode.
SW2(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name

`SW2(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws`	Configuring CFM domain over VPWS
`SW2(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none`	Creating MA for domain
`SW2(config-ether-cfm-mpls-md-ma)#cc interval 3`	Configuring CFM interval
`SW2(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 1`	Configuring remote mep
`SW2(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 4001 active true vpws ETH-2001`	Configuring local mep and mapping the same with vpws service
`SW2(config-ether-cfm-mpls-ma-mep)#cc multicast state enable`	Enabling the CFM multicast
`SW2(config-ether-cfm-mpls-ma-mep)#end`	Exit config mode
`SW2#conf t`	Config mode
`SW2(config)#ethernet cfm loss-measurement profile-name DM`	Configuring DM profile
`SW2(config-cfm-dm)#measurement interval`	Configuring measurement interval
`SW2(config-cfm-dm)# number-intervals-stored 3`	Configuring the number of history interval to be stored
`SW2(config-cfm-dm)# message-period 1s`	Configuring message period interval time
`SW2(config-cfm-dm)# bins-per-fd-interval 4`	Configuring the number of measurement bins per Measurement Interval for Frame Delay measurements.
`SW2(config-cfm-dm)# bins-per-ifdv-interval 3`	Configuring the number of measurement bins per Measurement Interval for Inter-Frame Delay Variation measurements.
`SW2(config-cfm-dm)#end`	Exit config mode

SW3

`SW3#configure terminal`	Enter configure mode.
`SW3(config)#interface xe17`	Configure interface
`SW3(config-if)#no switchport`	Configure interface as router port.
`SW3(config-if)#ip address 20.0.0.1/24`	Assign IP address to router port
`SW3(config-if)#no shutdown`	Making the interface up
`SW3(config-if)#exit`	Exit interface mode.
`SW3(config)#interface xe1`	Configure interface
`SW3(config-if)#no switchport`	Configure interface as router port.
`SW3(config-if)#ip address 10.0.0.2/24`	Assign IP address to router port
`SW3(config-if)#no shutdown`	Making the interface up
`SW3(config-if)#exit`	Exit interface mode.
`SW3(config)#interface lo`	Configure interface lo
`SW3(config-if)#ip address 2.2.2.2/32 secondary`	Configure secondary IP address to loopback interface .
`SW3(config-if)#exit`	Exit interface mode.

SW3(config)#router ospf 100	Configure ospf
SW3(config-router)#network 10.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW3(config-router)#network 2.2.2.2/32 area 0	Advertising loopback IP
SW3(config-router)#exit	Exit router mode.
SW3(config)#router rsvp	Configuring rsvp
SW3(config-router)#hello-receipt	Configuring hello reception
SW3(config-router)#no-php	Configuring device as not a PHP
SW3(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW3(config-router)#exit	Exit router mode.
SW3(config)#interface xe1	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.
SW3(config)#interface xe17	Configuring interface
SW3(config-if)#enable-rsvp	Enabling RSVP in interface
SW3(config-if)#label-switching	Enabling MPLS labeling
SW3(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW3(config-if)#exit	Exit interface mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#interface xe9	Configure interface
SW4(config-if)#switchport	Configure interface as switch port.
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface xe1	Configure interface
SW4(config-if)#no switchport	Configure interface as router port.
SW4(config-if)#ip address 20.0.0.2/24	Assign IP address to router port
SW4(config-if)#no shutdown	Making the interface up
SW4(config-if)#exit	Exit interface mode.
SW4(config)#interface lo	Configure interface lo
SW4(config-if)#ip address 3.3.3.3/32 secondary	Configure secondary IP address to loopback interface .
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ospf 100	Configure ospf
SW4(config-router)#network 20.0.0.0/24 area 0	Advertising 10 network
SW4(config-router)#network 3.3.3.3/32 area 0	Advertising loopback IP
SW4(config-router)#exit	Exit router mode.

SW4(config)#router rsvp	Configuring rsvp
SW4(config-router)#hello-receipt	Configuring hello reception
SW4(config-router)#no-php	Configuring device as not a PHP
SW4(config-router)#revert-timer 10	Configuring reversion time of RSVP
SW4(config-router)#exit	Exit router mode.
SW4(config)#rsvp-trunk to-1 ipv4	Configuring RSVP path
SW4(config-trunk)#to 2.2.2.2	Configuring first hop
SW4(config-trunk)#to 1.1.1.1	Configuring second hop
SW4(config-trunk)#exit	Exit trunk mode.
SW4(config)#interface xe1	Configuring interface
SW4(config-if)#enable-rsvp	Enabling RSVP in interface
SW4(config-if)#label-switching	Enabling MPLS labeling
SW4(config-if)#enable-ldp ipv4	Enabling ldp on interface
SW4(config-if)#exit	Exit interface mode.
SW4(config)#router ldp	Configuring LDP
SW4(config-router)#targeted-peer ipv4 1.1.1.1	Configuring LDP target peer for PW
SW4(config-router-targeted-peer)#exit-targeted-peer-mode	Exit target peer mode
SW4(config-router)#no multicast-hellos	Disabling LDP multicast
SW4(config-router)#exit	Exit router mode.
SW4(config)#mpls l2-circuit ETH-2001 1 1.1.1.1	Creating VPWS PW
SW4(config)#service-template ETH-2001	Configuring service template profile for PW
SW4(config-svc)# match outer-vlan 200	Configuring match condition
SW4(config-svc)# rewrite ingress push 2000	Configuring action for match
SW4(config-svc)#exit	Exit service template mode
SW4(config)#interface xe9	Configuring interface
SW4(config-if)#mpls-l2-circuit ETH-2001 service-template ETH-2001	Mapping VPWS in AC
SW4(config-if)#exit	Exit interface mode.
SW4(config)#hardware-profile filter cfm-domain-name-str enable	Enabling HW filter for character string domain name
SW4(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none vpws	Configuring CFM domain over VPWS
SW4(config-ether-cfm-mpls-md)#service ma-type string ma-name 43981 mip-creation none	Creating MA for domain
SW4(config-ether-cfm-mpls-md-ma)#cc interval 3	Configuring CFM interval
SW4(config-ether-cfm-mpls-md-ma)#mep cross-check mpid 4001	Configuring remote mep
SW4(config-ether-cfm-mpls-md-ma)#ethernet cfm mep up mpid 1 active true vpws ETH-2001	Configuring local mep and mapping the same with vpws service

SW4(config-ether-cfm-mpls-ma-mep)#cc multicast state enable	Enabling the CFM multicast
SW4(config-ether-cfm-mpls-ma-mep)#ethernet cfm loss-measurement reply dmm	Configuring DMR
SW4(config-ether-cfm-mpls-ma-mep)#end	Exit config mode

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering VLAN database.
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit config mode.
SW5(config)#interface xe9	Configure interface ce49.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1	Configure interface in bridge group 1
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface ce49.
SW5(config-if)#exit	Exit config mode.

Commands to initiate/abort delay measurement

```
delay-measurement type proactive profile-name WORD rmep (mac-address MAC|mep-id MEPID) mep MEPID domain DOMAIN_NAME (((vlan <2-4094>|) bridge <1-32>) | (vpws VCNAME))


abort delay-measurement mep MEPID domain DOMAIN_NAME (((vlan <2-4094>|) bridge <1-32>) | (vpws VCNAME)
```

Validation

```
SW2# delay-measurement type proactive profile-name DM rmep mac-address 3c2c.9926.e683 mep 200 domain 12345 vpws ETH-2001
SW2# show ethernet cfm delay-measurement mep 200 domain 12345 vpws ETH-2001
MD : 12345
MA : 43981
MEP : 200
VLAN ID : 0
VC Name : ETH-2001
Peer MAC Address : b86a.97d2.27d0
CURRENT:
======================
RMEP ID                  : 100
Measurement ID           : 3
Measurement Type         : DMM
Elapsed time(sec)        : 25
Start Time               : 2019 Nov 06 10:57:33
```

```
Suspect Flag                : TRUE
Min Frame Delay(usec)       : 37
Max Frame Delay(usec)       : 65
Avg Frame Delay(usec)       : 51
Min Inter FD Variation(usec): 13
Max Inter FD Variation(usec): 15
Avg Inter FD Variation(usec): 14
FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 3
2 5000 - < 9999 0
3 10000 - < 14999 0
4 15000 - < Inf 0
INTER-FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 2
2 5000 - < 9999 0
3 10000 - < Inf 0
HISTORY STATISTICS
======================
MD : 12345
MA : 43981
MEP : 200
VLAN ID : 0
VC Name : ETH-2001
RMEP ID : 100
Measurement ID : 1
Measurement Type : DMM
Elapsed time(sec) : 60
End Time : 2019 Nov 06 10:50:19
Suspect Flag : FALSE
Min Frame Delay(usec) : 14
Max Frame Delay(usec) : 75
Avg Frame Delay(usec) : 47
Min Inter FD Variation(usec): 53
Max Inter FD Variation(usec): 53
Avg Inter FD Variation(usec): 24
FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 5
2 5000 - < 9999 0
3 10000 - < 14999 0
4 15000 - < Inf 0
INTER-FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 4
```

```
2 5000 - < 9999 0
3 10000 - < Inf 0
RMEP ID : 100
Measurement ID : 2
Measurement Type : DMM
Elapsed time(sec) : 60
End Time : 2019 Nov 06 10:51:20
Suspect Flag : FALSE
Min Frame Delay(usec) : 13
Max Frame Delay(usec) : 70
Avg Frame Delay(usec) : 37
Min Inter FD Variation(usec): 52
Max Inter FD Variation(usec): 52
Avg Inter FD Variation(usec): 21
FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 6
2 5000 - < 9999 0
3 10000 - < 14999 0
4 15000 - < Inf 0
INTER-FRAME DELAY BINS
Bin Number Bin Threshold(usec) Bin Counter
================================================
1 0 - < 4999 5
2 5000 - < 9999 0
3 10000 - < Inf 0

SW1# abort delay-measurement mep 2 domain mdnam vlan 512 bridge 1
```

CHAPTER 5 G.8032 ERPS Version 2

G.8032 is an International Telecommunication Union (ITU) standard for ERPS. It prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

G.8032 Version 2 provides enhancements in support of multiple ring and ladder topologies. G.8032 offers a rapid detection and recovery time if a link or node.

This guide contains topologies and examples on how to configure g8032 ERPS configuration.

Topology

Figure 5-90 displays a sample Ring Protection topology on which protection switching is configured with four bridges. The Ring Protection Link (RPL) owner is the link between Bridge 3 and Bridge 4 (xe16), on which one side of the link is defined explicitly as RPL owner (Bridge 4) and RPL neighbor (Bridge 3). The rest of the bridges are explicitly configured RPL non owner to enable ERPS in the ring.

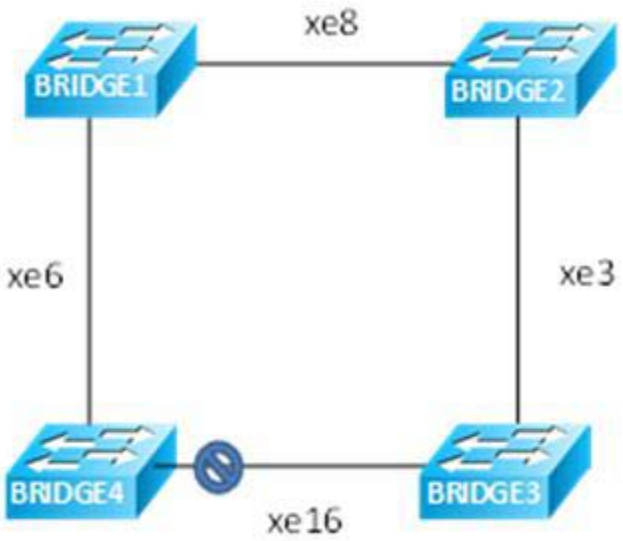


Figure 5-90: Major Ring Topology

Bridge 1

`Bridge1#configure terminal`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1

`Bridge1(config-vlan)#interface xe6`	Configure interface xe6
`Bridge1(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe6 interface
`Bridge1(config-if)#interface xe8`	Configure interface xe8
`Bridge1(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe8 interface
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 200 xe8`	Create down mep 12 with local vid 200 for xe8 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 14 active true local-vid 200 xe6`	Create down mep 14 with local vid 200 for xe6 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 41`	Configure crosscheck to remote MEP with value 41
`Bridge1(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge1(g8032-ring-config)#east-interface xe6`	Associate xe6 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface xe8`	Associate xe8 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge1(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge1(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 2

`Bridge2#config terminal`	Enter configure mode
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge2(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1

`Bridge2(config-vlan)#interface xe3`	Configure interface xe3
`Bridge2(config-if)#switchport`	Configure xe3 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe3 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe8 interface
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 xe3`	Create down mep 23 with local vid 200 for xe3 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 200 xe8`	Create down mep 21 with local vid 200 for xe8 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe8`	Associate xe8 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface xe3`	Associate xe3 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config terminal`	Enter configure mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config-vlan)#interface xe3`	Configure interface xe3

`Bridge3(config-if)#switchport`	Configure xe3 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe3 interface
`Bridge3(config-if)#interface xe16`	Configure interface xe16
`Bridge3(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe16 interface
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 xe3`	Create down mep 32 with local vid 200 for xe3 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 xe16`	Create down mep 34 with local vid 200 for xe16 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43
`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1

`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge3(g8032-ring-config)#east-interface xe3`	Associate xe3 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface xe16`	Associate xe16 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge3(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge3(g8032-config-switch)#rpl role neighbor west-interface`	Configure RPL node as neighbor node on west-interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configure mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge4(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config-vlan)#interface xe6`	Configure interface xe6
`Bridge4(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1

`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe6 interface
`Bridge4(config-if)#interface xe16`	Configure interface xe16
`Bridge4(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe16 interface
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 xe16`	Create down mep 43 with local vid 200 for xe16 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 41 active true local-vid 200 xe6`	Create down mep 41 with local vid 200 for xe6 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 14`	Configure crosscheck to remote MEP with value 14
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode

`Bridge4(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge4(g8032-ring-config)#east-interface xe16`	Associate xe16 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface xe6`	Associate xe6 interface as west-interface
`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge4(g8032-config-switch)#rpl role owner east-interface`	Configure the node as owner node on east-interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1:
show g8032 aps-statistics erp1 bridge 1

Instance   : erp1
==========
Tx   : 3205
Rx   : 27

show g8032 physical-ring RING1 bridge 1

Ring          : RING1
===============
Description   :
East          : xe16
West          : xe6
ERP Inst      : erp1
```

```
show g8032 profile profile1 bridge 1

Profile : profile1
=========
 Wait-To-Restore : 1 mins
 Hold Off Timer  : 0.00 secs
 Guard Timer     : 10 ms
 Wait-To-Block   : 5010 ms
 Protection Type : Revertive

Bridge1:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe6                 xe8
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:11   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod41               nod12
MEP ID          :  14                  12
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge2:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : d8:9e:f3:5e:f8:29
------------------------------------------------------------
                   East Link           West Link
============================================================
```

```
Interface       :  xe8                  xe3
State           :  Unblocked            Unblocked
Remote NodeId   :  34:17:eb:e4:af:11    -
Remote BPR      :  1                    -
Endpoint Info
-------------
Domain Name     :  nod12                nod23
MEP ID          :  21                   23
MA Name         :  43982                43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

sBridge3:
show g8032 erp-instance erp1 bridge 1
Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  xe3                  xe16
State           :  Unblocked            Blocked
Remote NodeId   :  34:17:eb:e4:af:11    34:17:eb:e4:af:11
Remote BPR      :  1                    1
Endpoint Info
-------------
Domain Name     :  nod23                nod34
MEP ID          :  32                   34
MA Name         :  43982                43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
```

```
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : OWNER (EAST)
Node ID         : 34:17:eb:e4:af:11
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  xe16                 xe6
State           :  Blocked              Unblocked
Remote NodeId   :  -                    -
Remote BPR      :  -                    -
Endpoint Info
-------------
Domain Name     :  nod34                nod41
MEP ID          :  43                   41
MA Name         :  43982                43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1
```

Sub-ring with Virtual Channel

An ethernet ring that is connected to a Major Ring at the Interconnection Nodes. By itself, the Sub-Ring does not constitute a closed ring. A Sub-Ring is connected to the Interconnection nodes on only one port which is configured as east-interface.

Topology

Figure 5-91 displays a sample Ring Protection topology on which protection switching is configured with six bridges. This constitutes of one major ring (Bridge2, Bridge3, Bridge4 and Bridge 5) and one sub-ring (Bridge2, Bridge1, Bridge6 and Bridge5).

Major ring's RPL in enabled between Bridge 3(owner node) and Bridge 4(neighbor node) on xe4 and other devices are non-owner nodes for that ring. Sub-ring's RPL is enabled between bridge 1(owner node) and bridge 2 (neighbor node) on link xe2 and other devices on the non-owner nodes. Bridge 2 and Bridge 5 are called interconnected nodes since they are common node between major ring and subring. Virtual channel is enabled for this Subring on interconnected nodes on vlan 100 and tcn propagation is enabled.

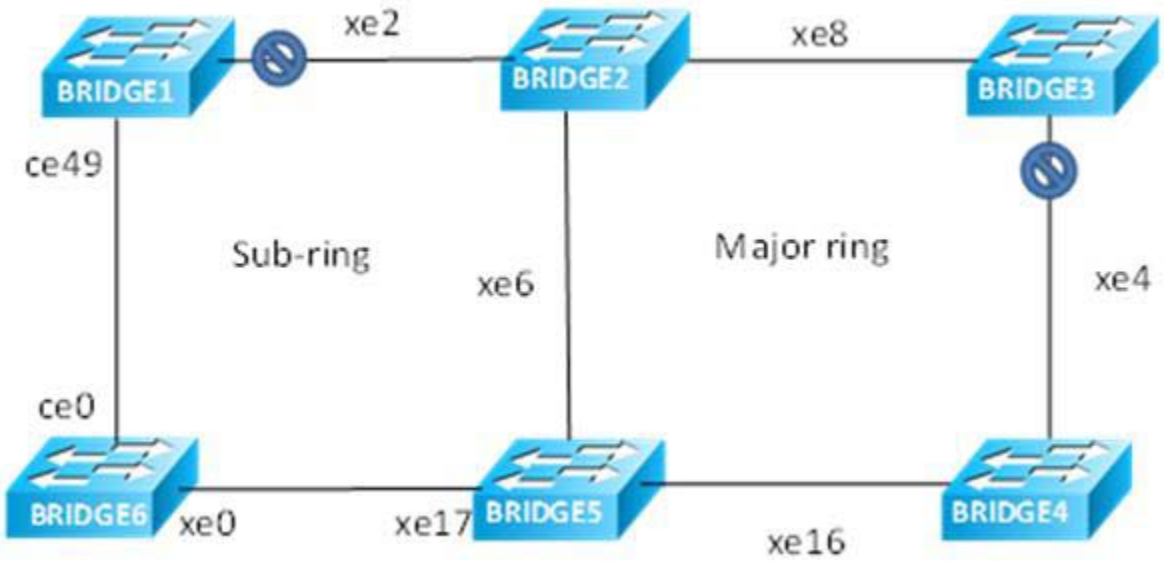


Figure 5-91: Major ring and Sub-ring with Virtual Channel Topology

Bridge 1

`Bridge1#config term`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge1(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge1(config)#interface ce49`	Configure interface ce49
`Bridge1(config-if)#switchport`	Configure ce49 as a layer 2 port

`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on ce49 interface
`Bridge1(config-if)#interface xe2`	Configure interface xe2
`Bridge1(config-if)#switchport`	Configure xe2 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe2 interface
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name 00061 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00061 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 16 active true local-vid 201 ce49`	Create down mep 16 with local vid 201 for ce49 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 61`	Configure crosscheck to remote MEP with value 61
`Bridge1(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00012 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00012 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 201 xe2`	Create down mep 12 with local vid 201 for xe2 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1

`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge1(g8032-ring-config)#east-interface ce49`	Associate ce49 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface xe2`	Associate xe2 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge1(g8032-config-switch)#ring-type sub-ring`	Configure ring type as subring
`Bridge1(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge1(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west-interface
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge1(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1

Bridge 2

`Bridge2#config term`	Enter configure mode
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge2(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge2(config)#interface xe2`	Configure interface xe2
`Bridge2(config-if)#switchport`	Configure xe2 as a layer 2 port

`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe2 interface
`Bridge2(config-if)#interface xe6`	Configure interface xe6
`Bridge2(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe6 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe8 interface
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name 00012 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00012 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 201 xe2`	Create down mep 21 with local vid 201 for xe2 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00052 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00052 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 25 active true local-vid 200 xe6`	Create down mep 25 with local vid 200 for xe6 interface

`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 52`	Configure crosscheck to remote MEP with value 52
`Bridge2(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00023 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 xe8`	Create down mep 23 with local vid 200 for xe8 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe6`	Associate xe6 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface xe8`	Associate xe8 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring ring`	Associate Physical ring RING1 to erp1 instance
`Bridge2(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring

`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe2`	Associate xe2 interface as east-interface
`Bridge2(g8032-ring-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge2(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge2(g8032-config-switch)#physical-ring subring`	Associate Physical ring RING1 to erp2 instance
`Bridge2(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge2(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure virtual channel with vlan 100 and attach erp2 to erp1
`Bridge2(g8032-config-switch)#tcn-propogation enable`	Enable tcn propogation
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config term`	Enter configure mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string

`Bridge3(config)#interface xe8`	Configure interface xe8
`Bridge3(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe8 interface
`Bridge3(config-if)#interface xe4`	Configure interface xe4
`Bridge3(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe4 interface
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name 00023 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 xe8`	Create down mep 32 with local vid 200 for xe8 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00034 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00034 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 xe4`	Create down mep 34 with local vid 200 for xe4 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43

`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge3(g8032-ring-config)#east-interface xe8`	Associate xe8 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface xe4`	Associate xe4 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge3(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge3(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge3(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configuration mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge5(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string

`Bridge4(config)#interface xe4`	Configure interface xe4
`Bridge4(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe4 interface
`Bridge4(config-if)#interface xe16`	Configure interface xe16
`Bridge4(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe16 interface
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name 00034 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 xe4`	Create down mep 43 with local vid 200 for xe4 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00045 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00045 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 45 active true local-vid 200 xe16`	Create down mep 45 with local vid 200 for xe16 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 54`	Configure crosscheck to remote MEP with value 54

`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge4(g8032-ring-config)#east-interface xe4`	Associate xe4 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface xe16`	Associate xe16 interface as west-interface
`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge4(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge4(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 5

`Bridge5#config term`	Enter configure mode
`Bridge5(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge5(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge5(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge5(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string

`Bridge5(config)#interface xe16`	Configure interface xe16
`Bridge5(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe16 interface
`Bridge5(config-if)#interface xe6`	Configure interface xe6
`Bridge5(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe6 interface
`Bridge5(config-if)#interface xe17`	Configure interface xe17
`Bridge5(config-if)#switchport`	Configure xe17 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe17 interface
`Bridge5(config-if)#ethernet cfm domain-type character-string domain-name 00045 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00045 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 54 active true local-vid 200 xe16`	Create down mep 54 with local vid 200 for xe16 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 45`	Configure crosscheck to remote MEP with value 45
`Bridge5(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00052 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00052 and set mip creation criteria to default with level 7 on bridge 1

`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 52 active true local-vid 200 xe6`	Create down mep 52 with local vid 200 for xe6 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 25`	Configure crosscheck to remote MEP with value 25
`Bridge5(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00056 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00056 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 56 active true local-vid 201 xe17`	Create down mep 56 with local vid 201 for xe17 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 65`	Configure crosscheck to remote MEP with value 65
`Bridge5(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge5(g8032-ring-config)#east-interface xe16`	Associate xe16 interface as east-interface
`Bridge5(g8032-ring-config)#west-interface xe6`	Associate xe6 interface as west-interface
`Bridge5(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge5(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge5(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge5(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge5(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode

`Bridge5(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge5(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge5(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge5(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge5(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge5(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge5(g8032-config-switch)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge5(g8032-ring-config)#east-interface xe17`	Associate xe17 interface as east-interface
`Bridge5(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge5(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge5(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge5(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge5(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge5(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge5(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure virtual channel with vlan 100 and attach erp2 to erp1
`Bridge5(g8032-config-switch)#tcn-propogation enable`	Enable tcn propogation
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 6

`Bridge6#config term`	Enter configuration mode
`Bridge6(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.

`Bridge6(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge6(config-vlan)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge6(config)#interface xe0`	Configure interface xe0
`Bridge6(config-if)#switchport`	Configure xe0 as a layer 2 port
`Bridge6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge6(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge6(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge6(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe0 interface
`Bridge6(config-if)#interface ce0`	Configure interface ce0
`Bridge6(config-if)#switchport`	Configure ce0 as a layer 2 port
`Bridge6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge6(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge6(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge6(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on ce0 interface
`Bridge6(config-if)#ethernet cfm domain-type character-string domain-name 00056 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00056 and set mip creation criteria to default with level 7 on bridge 1
`Bridge6(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201.
`Bridge6(config-ether-cfm-ma)#ethernet cfm mep down mpid 65 active true local-vid 201 xe0`	Create down mep 65 with local vid 201 for xe0 interface
`Bridge6(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge6(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge6(config-ether-cfm-ma)#mep crosscheck mpid 56`	Configure crosscheck to remote MEP with value 56
`Bridge6(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge6(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge6(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00061 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00061 and set mip creation criteria to default with level 7 on bridge 1
`Bridge6(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge6(config-ether-cfm-ma)#ethernet cfm mep down mpid 61 active true local-vid 201 ce0`	Create down mep 61 with local vid 201 for ce0 interface
`Bridge6(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast

`Bridge6(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge6(config-ether-cfm-ma)#mep crosscheck mpid 16`	Configure crosscheck to remote MEP with value 16
`Bridge6(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge6(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge6(config-ether-cfm)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge6(g8032-ring-config)#east-interface xe0`	Associate xe0 interface as east-interface
`Bridge6(g8032-ring-config)#west-interface ce0`	Associate ce0 interface as west-interface
`Bridge6(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge6(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge6(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge6(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge6(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge6(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge6(g8032-config-switch)#ring-type sub-ring`	Configure ring type as subring
`Bridge6(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge6(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge6(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge6(g8032-config-switch)#level 7`	Configure level as 7
`Bridge6(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge6(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge6(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge6(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING
```

```
Role            : OWNER (WEST)
Node ID         : 6c:b9:c5:67:72:1d
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  ce49                xe2
State           :  Unblocked           Blocked
Remote NodeId   :  -                   -
Remote BPR      :  -                   -
Endpoint Info
-------------
Domain Name     :  00061               00012
MEP ID          :  16                  12
MA Name         :  43982               43982
=======================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge2#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING (VIRTUAL)
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:26:e6:7c
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe2                 -
State           :  Blocked             -
Remote NodeId   :  6c:b9:c5:67:72:1d   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  00012               -
MEP ID          :  21                  -
MA Name         :  43982               -
=======================================================
TCN Propagation : Enabled
Attached        : -
Attached To     : erp1,
Virtual ID      : 100 : 1
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
```

```
============================

DataTraffic vlan: 202-205
Profile : profile1


Bridge2#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  xe6                  xe8
State           :  Unblocked            Unblocked
Remote NodeId   :  -                    d8:9e:f3:5e:f8:29
Remote BPR      :  -                    0
Endpoint Info
-------------
Domain Name     :  00052                00023
MEP ID          :  25                   23
MA Name         :  43982                43982
============================================================
TCN Propagation : Disabled
Attached        : erp2,
Attached To     : -
Virtual ID      : -:-
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge3#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : OWNER (WEST)
Node ID         : d8:9e:f3:5e:f8:29
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  xe8                  xe4
State           :  Unblocked            Blocked
```

```
Remote NodeId   :  -                    -
Remote BPR      :  -                    -
Endpoint Info
-------------
Domain Name     :  00023                00034
MEP ID          :  32                   34
MA Name         :  43982                43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge4#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:1a:da:7e
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe4                  xe16
State           :  Blocked              Unblocked
Remote NodeId   :  d8:9e:f3:5e:f8:29    d8:9e:f3:5e:f8:29
Remote BPR      :  0                    0
Endpoint Info
-------------
Domain Name     :  00034                00045
MEP ID          :  43                   45
MA Name         :  43982                43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge5#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
```

```
Phy Ring        : subring
Ring Type       : SUB-RING (VIRTUAL)
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:12
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe17                -
State           :  Unblocked           -
Remote NodeId   :  6c:b9:c5:67:72:1d   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  00056               -
MEP ID          :  56                  -
MA Name         :  43982               -
=======================================================
TCN Propagation : Enabled
Attached        : -
Attached To     : erp1,
Virtual ID      : 100 : 1
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge5#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:11
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe16                xe6
State           :  Unblocked           Unblocked
Remote NodeId   :  -                   d8:9e:f3:5e:f8:29
Remote BPR      :  -                   0
Endpoint Info
-------------
Domain Name     :  00045               00052
MEP ID          :  54                  52
MA Name         :  43982               43982
=======================================================
TCN Propagation : Disabled
Attached        : erp2,
Attached To     : -
```

```
Virtual ID      : -:-
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge6#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING
Role            : NON-OWNER
Node ID         : b8:6a:97:d2:27:c6
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe0                 ce0
State           :  Unblocked           Unblocked
Remote NodeId   :  -                   6c:b9:c5:67:72:1d
Remote BPR      :  -                   0
Endpoint Info
-------------
Domain Name     :  00056               00061
MEP ID          :  65                  61
MA Name         :  43982               43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    201,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1
```

Sub-ring without Virtual Channel on a LAG interface

Figure 3 displays a sample Ring Protection topology on which protection switching is configured with 5 bridges on lag interfaces. The topology contains one major ring and one subring with non-virtual channel. The Ring Protection Link (RPL) for major ring is the link between Bridge 4 (owner) and Bridge 3 (neighbor) on lag interface po3. The subring is configured with no virtual channel and it's RPL link is configured between bridge 1 (neighbor) and bridge 5 (owner) on lag interface po6. The rest of the bridges are explicitly configured RPL non owner to enable ERPS in the ring in both major and subring.

Topology

Figure 5-92 displays a sample Ethernet Ring Protection Switching topology.

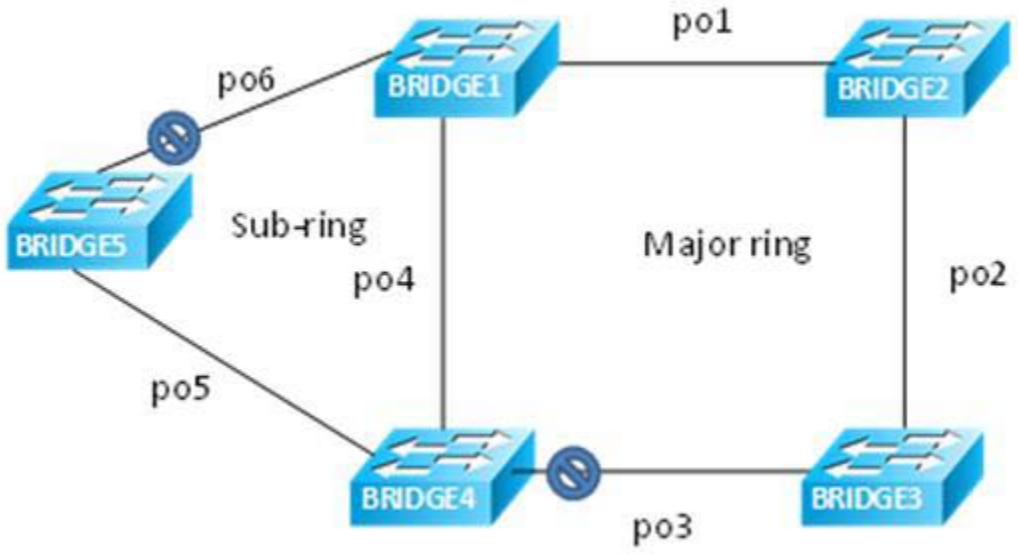


Figure 5-92: Major ring and sub-ring topology using LAG interface without a virtual channel

Bridge 1

`Bridge1#config term`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge1(config-vlan)#interface po1`	Configure lag interface po1
`Bridge1(config-if)#switchport`	Configure po1 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port

`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po1 interface
`Bridge1(config-if)#interface po4`	Configure lag interface po4
`Bridge1(config-if)#switchport`	Configure po4 as a layer 2 port
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Configure interface in bridge group 1
`Bridge1(config-if)#switchport mode trunk`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po4 interface
`Bridge1(config-if)#interface po6`	Configure lag interface po6
`Bridge1(config-if)#switchport`	Configure po6 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po6 interface
`Bridge1(config-if)#interface xe1`	Configure interface xe1
`Bridge1(config-if)#channel-group 6 mode active`	Configure xe1 as part of po6
`Bridge1(config-if)#interface xe2`	Configure interface xe2
`Bridge1(config-if)#channel-group 6 mode active`	Configure xe2 as part of po6
`Bridge1(config-if)#interface xe6`	Configure interface xe6
`Bridge1(config-if)#channel-group 4 mode active`	Configure xe6 as part of po4
`Bridge1(config-if)#interface xe7`	Configure interface xe7
`Bridge1(config-if)#channel-group 4 mode active`	Configure xe7 as part of po4
`Bridge1(config-if)#interface xe8`	Configure interface xe8
`Bridge1(config-if)#channel-group 1 mode active`	Configure xe8 as part of po1
`Bridge1(config-if)#interface xe9`	Configure interface xe9
`Bridge1(config-if)#channel-group 1 mode active`	Configure xe9 as part of po1
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 200 po1`	Create down mep 12 with local vid 200 for po1 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 14 active true local-vid 200 po4`	Create down mep 14 with local vid 200 for po4 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 41`	Configure crosscheck to remote MEP with value 41
`Bridge1(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod15 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod15 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 51 active true local-vid 200 po6`	Create down mep 51 with local vid 200 for po6 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 15`	Configure crosscheck to remote MEP with value 15
`Bridge1(config-ether-cfm-ma)#cc interval 1`	Enable cc interval with 1
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge1(g8032-ring-config)#east-interface po4`	Associate po4 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface po1`	Associate po1 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min

`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge1(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge1(g8032-config-switch)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge1(g8032-ring-config)#east-interface po6`	Associate po6 interface as east-interface
`Bridge1(g8032-ring-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge1(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge1(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge1(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge1(g8032-config-switch)# tcn-propogation enable`	Enable tcn propogation
`Bridge1(g8032-config-switch)# tcn-to-instance erp1`	Attach erp1 instance to erp2 instance to notify any changes in subring to major ring
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 2

`Bridge2#config term`	Enter configure mode
`Bridge2(config)#hardware-profile filter cfm-domain-name-str enable`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Enable CFM domain name as string
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge2(config-vlan)#interface po1`	Configure lag interface po1
`Bridge2(config-if)#switchport`	Configure po1 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po1 interface
`Bridge2(config-if)#interface po2`	Configure lag interface po2
`Bridge2(config-if)#switchport`	Configure po2 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po2 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#channel-group 1 mode active`	Configure xe8 as part of po1
`Bridge2(config-if)#interface xe9`	Configure interface xe9
`Bridge2(config-if)#channel-group 1 mode active`	Configure xe9 as part of po1
`Bridge2(config-if)#interface xe3`	Configure interface xe3
`Bridge2(config-if)#channel-group 2 mode active`	Configure xe3 as part of po2
`Bridge2(config-if)#interface xe4`	Configure interface xe4
`Bridge2(config-if)#channel-group 2 mode active`	Configure xe4 as part of po2
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 200 po1`	Create down mep 21 with local vid 200 for po1 interface

`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 po2`	Create down mep 23 with local vid 200 for po2 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge2(g8032-ring-config)#east-interface po1`	Associate po1 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface po2`	Associate po2 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node

`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config term`	Enter configuration mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config-vlan)#interface po2`	Configure lag interface po2
`Bridge3(config-if)#switchport`	Configure po2 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po2 interface
`Bridge3(config-if)#interface po3`	Configure lag interface po3
`Bridge3(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge3(config-if)#interface xe3`	Configure interface xe3
`Bridge3(config-if)#channel-group 2 mode active`	Configure xe3 as part of po2
`Bridge3(config-if)#interface xe4`	Configure interface xe4
`Bridge3(config-if)#channel-group 2 mode active`	Configure xe4 as part of po2
`Bridge3(config-if)#interface xe15`	Configure interface xe3
`Bridge3(config-if)#channel-group 3 mode active`	Configure xe3 as part of po3
`Bridge3(config-if)#interface xe16`	Configure interface xe16

`Bridge3(config-if)#channel-group 3 mode active`	Configure xe16 as part of po3
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 po2`	Create down mep 32 with local vid 200 for po2 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 po3`	Create down mep 34 with local vid 200 for po3 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43
`Bridge3(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge3(g8032-ring-config)#east-interface po2`	Associate po2 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface po3`	Associate po3 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0

`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge3(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge3(g8032-config-switch)#rpl role neighbor west-interface`	Configure the node as neighbor node on west interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configure mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge4(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config-vlan)#interface po3`	Configure lag interface po3
`Bridge4(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge4(config-if)#interface po4`	Configure lag interface po4
`Bridge4(config-if)#switchport`	Configure po4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po4 interface
`Bridge4(config-if)#interface po5`	Configure lag interface po5

`Bridge4(config-if)#switchport`	Configure po5 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po5 interface
`Bridge4(config-if)#interface xe6`	Configure interface xe6
`Bridge4(config-if)#channel-group 4 mode active`	Configure xe6 as part of po4
`Bridge4(config-if)#interface xe7`	Configure interface xe7
`Bridge4(config-if)#channel-group 4 mode active`	Configure xe7 as part of po4
`Bridge4(config-if)#interface xe10`	Configure interface xe10
`Bridge4(config-if)#channel-group 5 mode active`	Configure xe10 as part of po5
`Bridge4(config-if)#interface xe11`	Configure interface xe11
`Bridge4(config-if)#channel-group 5 mode active`	Configure xe11 as part of po5
`Bridge4(config-if)#interface xe15`	Configure interface xe15
`Bridge4(config-if)#channel-group 3 mode active`	Configure xe15 as part of po3
`Bridge4(config-if)#interface xe16`	Configure interface xe16
`Bridge4(config-if)#channel-group 3 mode active`	Configure xe16 as part of po3
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 po3`	Create down mep 43 with local vid 200 for po3 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200

`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 41 active true local-vid 200 po4`	Create down mep 41 with local vid 200 for po4 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 14`	Configure crosscheck to remote MEP with value 14
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod45 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod45 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 54 active true local-vid 200 po5`	Create down mep 54 with local vid 200 for po5 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 45`	Configure crosscheck to remote MEP with value 45
`Bridge4(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge4(g8032-ring-config)#east-interface po3`	Associate po3 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface po4`	Associate po4 interface as west-interface
`Bridge4(g8032-ring-config)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge4(g8032-ring-config)#east-interface po5`	Associate po5 interface as east-interface
`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode

`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge4(g8032-config-switch)#rpl role owner east-interface`	Configure the node as owner node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge4(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge4(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge4(g8032-config-switch)#rpl role non-owner`	Configure the node as neighbor node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge4(g8032-config-switch)# tcn-propogation enable`	Enable tcn propogation
`Bridge4(g8032-config-switch)# tcn-to-instance erp1`	Attach erp1 instance to erp2 instance to notify any changes in subring to major ring
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 5

`Bridge5#config term`	Enter config mode
`Bridge5(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge5(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string
`Bridge5(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge5(config-vlan)#interface po5`	Configure lag interface po5
`Bridge5(config-if)#switchport`	Configure po5 as a layer 2 port

`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge5(config-if)#interface po6`	Configure lag interface po3
`Bridge5(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge5(config-if)#interface xe1`	Configure interface xe1
`Bridge5(config-if)#channel-group 6 mode active`	Configure xe1 as part of po6
`Bridge5(config-if)#interface xe2`	Configure interface xe2
`Bridge5(config-if)#channel-group 6 mode active`	Configure xe2 as part of po6
`Bridge5(config-if)#interface xe10`	Configure interface xe10
`Bridge5(config-if)#channel-group 5 mode active`	Configure xe10 as part of po5
`Bridge5(config-if)#interface xe11`	Configure interface xe11
`Bridge5(config-if)#channel-group 5 mode active`	Configure xe11 as part of po5
`Bridge5(config-if)#ethernet cfm domain-type character-string domain-name nod15 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod15 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 15 active true local-vid 200 po6`	Create down mep 15 with local vid 200 for po6 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 51`	Configure crosscheck to remote MEP with value 51
`Bridge5(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod45 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod45 and set mip creation criteria to default with level 7 on bridge 1

`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 45 active true local-vid 200 po5`	Create down mep 45 with local vid 200 for po5 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 54`	Configure crosscheck to remote MEP with value 54
`Bridge5(config-ether-cfm-ma)#cc  interval 1`	Enable cc interval with 1
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge5(g8032-ring-config)#east-interface po5`	Associate po5 interface as east-interface
`Bridge5(g8032-ring-config)#west-interface po6`	Associate po6 interface as west-interface
`Bridge5(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge5(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge5(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge5(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge5(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge5(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge5(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge5(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as subring
`Bridge5(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west interface
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge5(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge5(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING (NON VIRTUAL)
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:26:e6:7b
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  po6                  -
State           :  Blocked              -
Remote NodeId   :  6c:b9:c5:67:72:f6    -
Remote BPR      :  0                    -
Endpoint Info
-------------
Domain Name     :  nod15                -
MEP ID          :  51                   -
MA Name         :  43982                -
============================================================
TCN Propagation : Enabled
TCN Propagation List: erp1,

     Channel               |
 (LEVEL, VLAN, RING ID)    |
============================
 (7,    200,   2)          |
============================

Bridge1#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1ance erp2 bridge
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  po4                  po1
State           :  Unblocked            Unblocked
Remote NodeId   :  34:17:eb:e4:af:10    -
Remote BPR      :  1                    -
Endpoint Info
-------------
Domain Name     :  nod41                nod12
MEP ID          :  14                   12
MA Name         :  43982                43982
============================================================
```

```
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge2#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : d8:9e:f3:5e:f8:29
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po1                 po2
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:10   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod12               nod23
MEP ID          :  21                  23
MA Name         :  43982               43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge3#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po2                 po3
State           :  Unblocked           Blocked
Remote NodeId   :  34:17:eb:e4:af:10   34:17:eb:e4:af:10
```

```
Remote BPR      :  1                   1
Endpoint Info
-------------
Domain Name     :  nod23               nod34
MEP ID          :  32                  34
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING (NON VIRTUAL)
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:0b
------------------------------------------------------------
                    East Link           West Link
============================================================
Interface       :  po5                 -
State           :  Unblocked           -
Remote NodeId   :  6c:b9:c5:67:72:f6   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  nod45               -
MEP ID          :  54                  -
MA Name         :  43982               -
============================================================
TCN Propagation : Enabled
TCN Propagation List: erp1,

     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   2)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
```

```
Ring Type       : MAJOR-RING
Role            : OWNER (EAST)
Node ID         : 34:17:eb:e4:af:10
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po3                 po4
State           :  Blocked             Unblocked
Remote NodeId   :  -                   -
Remote BPR      :  -                   -
Endpoint Info
-------------
Domain Name     :  nod34               nod41
MEP ID          :  43                  41
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge5#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING
Role            : OWNER (WEST)
Node ID         : 6c:b9:c5:67:72:f6
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po5                 po6
State           :  Unblocked           Blocked
Remote NodeId   :  -                   -
Remote BPR      :  -                   -
Endpoint Info
-------------
Domain Name     :  nod45               nod15
MEP ID          :  45                  15
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   2)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1
```



```
Bridge3#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po2                 po3
State           :  Unblocked           Blocked
Remote NodeId   :  34:17:eb:e4:af:10   34:17:eb:e4:af:10
Remote BPR      :  1                   1
Endpoint Info
-------------
Domain Name     :  nod23               nod34
MEP ID          :  32                  34
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1
```

CHAPTER 6 Ethernet Test Signal Lock Configuration

ETH-TST (Ethernet Test Signal) and ETH-LCK (Ethernet Lock Signal) protocols are defined in Y.1731. ETH-TST is used to perform one-way on-demand in-service or out-of-service diagnostics tests. This includes verifying bandwidth throughput, frame loss, bit errors, etc.

ETH-LCK is used to communicate the administrative locking of a MEP and consequential interruption of data traffic forwarding towards the MEP expecting this traffic. It allows a MEP receiving frames with ETH-LCK information to differentiate between a defect condition and an administrative locking action at lower level MEP.

Topology

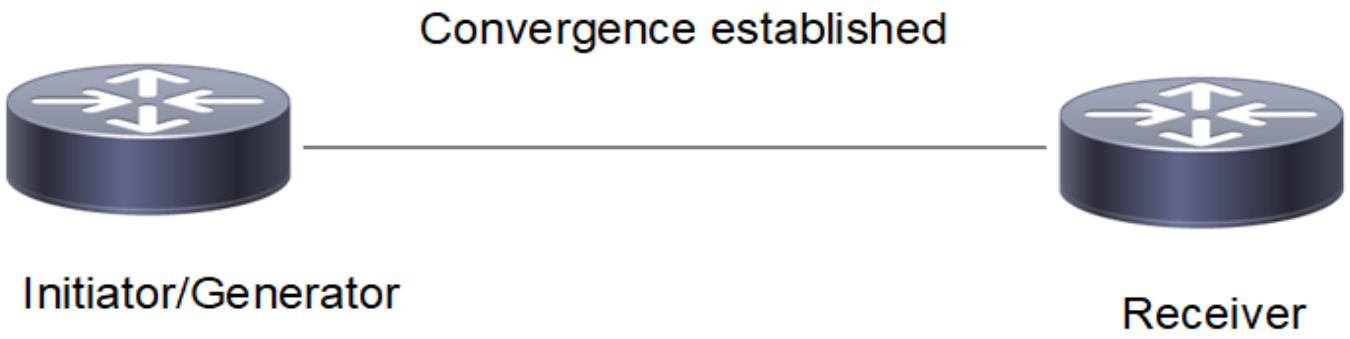


Figure 6-93: ETH Test Signal Topology

ETH-TST Configuration

Initiator/generator

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter cfm-domain-name-str enable`	Configure Hardware profile filter.
`(config)#hardware-profile statistics ingress-acl enable`	Configure hardware profile statistics ingress-acl.
`(config)#vlan database`	Enter Vlan config mode.
`(config-vlan)#vlan 2-100 bridge 1 state enable`	Configure Vlans.
`(config-vlan)#exit`	Exit Vlan config mode.
`(config)#interface xe15`	Enter Interface config mode.
`(config-if)#switchport`	Configure Interface as switchport.
`(config-if)#bridge-group 1`	Configure bridge-group.
`(config-if)#switchport mode trunk`	Configure switchport mode as trunk.
`(config-if)#switchport trunk allowed vlan all`	Configure all vlans as part of switchport trunk.
`(config-if)#no shutdown`	Bring the interface into operation.

(config-if)#exit	Exit interface mode.
(config)#ethernet cfm domain-type character-string domain-name test1 level 7 mip-creation none bridge 1	Enter ethernet cfm mode by specifying domain name and bridge.
(config-ether-cfm)#service ma-type string ma-name test1 vlan 10 mip-creation none	Configure service ma.
(config-ether-cfm-ma)#ethernet cfm mep down mpid 200 active true local-vid 10 xe15	Configure ethernet cfm mep.
(config-ether-cfm-ma-mep)#cc multicast state enable	Enable multicast state.
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit Ethernet ma mep mode.
(config-ether-cfm-ma)#mep crosscheck mpid 100	Configure RMEP.
(config-ether-cfm-ma)#cc interval 5	Configure interval in ma mode.
(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ma mode.
(config-ether-cfm)#exit	Exit Ethernet cfm mode.
(config)#ethernet cfm test-signal profile-name test	Configure Ethernet cfm test-signal profile.
(config-cfm-tst)#test-signal mode both	Configure test-signal mode as both(generator and receiver).
(config-cfm-tst)#test-signal frame-size 1500	Configure test-signal frame-size.
(config-cfm-tst)#exit	Exit Ethernet cfm test-signal mode.

Receiver

#configure terminal	Enter configure mode.
(config)#hardware-profile filter cfm-domain-name-str enable	Configure Hardware profile filter.
(config)#hardware-profile statistics ingress-acl enable	Configure hardware profile statistics ingress-acl.
(config)#vlan database	Enter Vlan config mode.
(config-vlan)#vlan 2-100 bridge 1 state enable	Configure Vlans.
(config-vlan)#exit	Exit Vlan config mode.
(config)#interface xe15	Enter Interface config mode.
(config-if)#switchport	Configure Interface as switchport.
(config-if)#bridge-group 1	Configure bridge-group.
(config-if)#switchport mode trunk	Configure switchport mode as trunk.
(config-if)#switchport trunk allowed vlan all	Configure all vlans as part of switchport trunk.
(config-if)#no shutdown	Bring the interface into operation.
(config-if)#exit	Exit interface mode.
(config)#ethernet cfm domain-type character-string domain-name test1 level 7 mip-creation none bridge 1	Enter ethernet cfm mode by specifying domain name and bridge.
(config-ether-cfm)#service ma-type string ma-name test1 vlan 10 mip-creation none	Configure service ma.

(config-ether-cfm-ma)#ethernet cfm mep down mpid 100 active true local-vid 10 xe15	Configure ethernet cfm mep.
(config-ether-cfm-ma-mep)#cc multicast state enable	Enable multicast state.
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit Ethernet ma mep mode.
(config-ether-cfm-ma)#mep crosscheck mpid 200	Configure RMEP.
(config-ether-cfm-ma)#cc interval 5	Configure interval in ma mode.
(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ma mode.
(config-ether-cfm)#exit	Exit Ethernet cfm mode.
(config)#ethernet cfm test-signal profile-name sample_tst	Configure Ethernet cfm test-signal profile.
(config-cfm-tst)#test-signal mode receiver	Configure test-signal mode as receiver.
(config-cfm-tst)#exit	Exit Ethernet cfm test-signal mode.

Validation

Before the ETH-TST signal is started, convergence needs to be established. Convergence is checked as mentioned below :

```
CE1#sh ethernet cfm errors domain test1 bridge 1
Domain Name         Level     Vlan     MEPID     Defects
-----------------------------------------------------------
test1               7         10       200       .....
1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM
```

After the above convergence is established with the receiver node, ETH-TST signal is started from the exec mode as mentioned below :

Generator node :

```
#test-signal start-time relative 0 stop-time relative 4 tst-profile-name test domain
test1 ma test1 mep 200 target mac-address 0018.236c.5cca  bridge 1
```

Receiver node :

```
#test-signal start-time relative 0 stop-time relative 4 tst-profile-name sample_tst
domain test1 ma test1 mep 100 target mac-address e8c5.7a78.712d  bridge 1
```

ETH-TST Signal initiated is checked as mentioned below :

Generator node :

```
#show ethernet cfm test-signal sessions
MEP-Id  Status    StartTime             Tst-Profile       Peer MAC-Address
-------------------------------------------------------------------------------
200     Active    2019/02/15 16:32:59     test            0018.236c.5cca


#show ethernet cfm test-signal domain test1 ma test1 mep 200 bridge 1 stats gtf
 TST Session status          : In-Progress
 Elapsed Time(sec)           : 77
 MD                        : test1
```

```
 MA                          : test1
 MEP                         : 200
 Peer MAC Address            : 0018.236c.5cca
 RMEP ID                     : 100
 Start Time                    : 2019 Feb 15 16:32:59
 Transmitted Packet Count     : 509767
```

Receiver Node :

```
#show ethernet cfm test-signal domain test1 ma test1 mep 100 bridge 1 stats ctf
 TST Session status          : In-Progress
 Elapsed Time(sec)           : 83
 MD                          : test1
 MA                          : test1
 MEP                         : 100
 Peer MAC Address            : e8c5.7a78.712d
 RMEP ID                     : 200
 Start Time                    : 2020 Dec 16 16:34:21
 Received Packet Count        : 545827
 Out-of-Order Packet Count     : 0
 Error Packet Count            : 0
 Last Packet Sequence Number : 664967
```

ETH-LCK Configuration

Eth-Lck configuration is performed at the MEP Level as shown below :

`#configure terminal`	Enter configure mode
`(config)# ethernet cfm domain-type character-string domain-name test1 level 7 mip-creation none bridge 1`	Enter ethernet cfm mode by specifying domain name and bridge.
`(config-ether-cfm)#service ma-type string ma-name test1 vlan 10 mip-creation none`	Configure service ma
`(config-ether-cfm-ma)#ethernet cfm mep down mpid 200 active true local-vid 10 xe15`	Configure ethernet cfm mep
`(config-ether-cfm-ma-mep)#`	Eth Lck configuration is performed in MEP Mode

Validation

Default state of the Ethernet cfm Lck details is as mentioned below :

```
#show ethernet cfm lck details domain test1 ma test1 mep 200 bridge 1

Maintenance Domain             : test1
Maintenance Association          : test1
MEP ID                         : 200
LCK PDU state                   : Unlocked
LCK Message Level              : 0
LCK PDU Interval                : 1 sec
LCK PDU Priority                : 3
```

```
(config-ether-cfm-ma-mep)#eth-lck state ?
  lock    Enable adminstrative locking state
  unlock  Disable adminstrative locking state

(config-ether-cfm-ma-mep)#eth-lck state lock
#show ethernet cfm lck details domain test1 ma test1 mep 200 bridge 1

Maintenance Domain              : test1
Maintenance Association           : test1
MEP ID                          : 200
LCK PDU state                 : Locked
LCK Message Level               : 0
LCK PDU Interval                 : 1 sec
LCK PDU Priority                 : 3

(config-ether-cfm-ma-mep)#eth-lck message level ?
  <0-7>  Enter the level for LCK transmission

(config-ether-cfm-ma-mep)#eth-lck message level 3
#show ethernet cfm lck details domain test1 ma test1 mep 200 bridge 1
Maintenance Domain              : test1
Maintenance Association           : test1
MEP ID                          : 200
LCK PDU state                    : Locked
LCK Message Level             : 3
LCK PDU Interval                  : 1 sec
LCK PDU Priority                  : 3

(config-ether-cfm-ma-mep)#eth-lck interval ?
one-minute  TX interval one minute
one-second  TX interval one second

(config-ether-cfm-ma-mep)#eth-lck interval one-minute
#show ethernet cfm lck details domain test1 ma test1 mep 200 bridge 1
Maintenance Domain              : test1
Maintenance Association           : test1
MEP ID                          : 200
LCK PDU state                    : Locked
LCK Message Level               : 3
LCK PDU Interval               : 1 min
LCK PDU Priority                  : 3

(config-ether-cfm-ma-mep)#eth-lck frame priority ?
<0-7>  Enter the priority for LCK transmission PDU

(config-ether-cfm-ma-mep)#eth-lck frame priority 7
#show ethernet cfm lck details domain test1 ma test1 mep 200 bridge 1
Maintenance Domain              : test1
Maintenance Association         : test1
```

```
MEP ID                          : 200
LCK PDU state                   : Locked
LCK Message Level               : 3
LCK PDU Interval                : 1 min
LCK PDU Priority                : 7
```

Carrier Ethernet Command Reference

Contents

This document contains these chapters and appendices:

CHAPTER 1 Link Layer Discovery Protocol v2 Commands

The commands in this chapter support:

- Link Layer Discovery Protocol (LLDP) version 2 as described in IEEE 802.1AB 2009
- LLDP-MED protocol extension as per ANSI/TIA-1057 April 2006.

Note: To enable LLDPv2, LLDP (previous version) should be disabled or vice versa.

clear lldp counters

Use this command to clear the LLDP statistics on all the interfaces.

Command Syntax

```
clear lldp counters
```

Parameters

`counters`	Reset the LLDP traffic counters to zero.

Command Mode

Exec Mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear lldp counters
```

lldp-agent

Use this command to create an LLDP agent mode.

Note: This command is not supported in SVLAN, VLAN, and loopback interfaces.

Use the no parameter to revert to default settings.

Command Syntax

```
lldp-agent (non-tpmr-bridge |customer-bridge| )
no lldp-agent (non-tpmr-bridge |customer-bridge| )
```

Parameters

`non-tpmr-bridge`
non-tpmr-bridge

`customer-bridge`
customer-bridge

Default

By default LLDP agent is disabled.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent customer-bridge
(if-lldp-agent)#

(if-lldp-agent)#no lldp-agent customer-bridge
(if-lldp-agent)#exit
(config-if)#
```

debug lldp

Use this command to set the debugging functions for LLDP.

Use the no form of this command to turn off LLDP debugging functions

Command Syntax

```
debug lldp (event|ha|rx|tx|message)
no debug lldp (event|ha|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`ha`	Enable or disable high availability debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging
`message`	Enable or disable NSM message debugging

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug lldp event
#debug lldp message
```

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP)

Use the no form of this command to stop LLDP

Command Syntax

```
lldp run
no lldp run
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lldp run

(config)#no lldp run
```

lldp tlv basic-mgmt

Use this command to select and unselect basic management TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the no parameter to remove the basic management TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name) (select|unselect)
no lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`	Management address TLV
`port-description`	Port description TLV
`system-capabilities`	System capabilities TLV
`system-description`	System Description TLV
`system-name`	System name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv basic-mgmt system-name select
(if-lldp-agent)#exit
```

lldp tlv med

Use this command to select and unselect Media Endpoint Devices (MED) TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

LLDP MED TLVs determine the capabilities the connected device supports and the capabilities the device has enabled.

Use the no parameter to remove the MED TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi) (select|unselect)
no lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi)
```

Parameters

`network-policy`	Network-policy TLV
`location`	Location TLV
`inventory`	Inventory TLV
`media-capabilities`	Media-capabilities TLV
`extended-power-via-mdi`	Extended-power-via-mdi TLV (when PoE is available)
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv med network-policy select
(if-lldp-agent)#exit
```

lldp tlv ieee-8021-org-specific

Use this command to select and unselect ieee-8021-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the no parameter to remove the ieee-8021-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-
  vlanid|ptcl-identity|vid-digest|vlan-name) (select|unselect)
no lldp tlv ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-
  identity|vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select
(if-lldp-agent)#exit
```

lldp tlv ieee-8023-org-specific

Use this command to select and unselect ieee-8023-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the no parameter to remove the ieee-8023-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
  (select|unselect)
no lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	Provider edge port VLAN ID TLV
`power-via-mdi`	Power-via-MDI TLV (when PoE is available)
`max-mtu-size`	Maximum MTU size TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select
(if-lldp-agent)#exit
```

lldp tlv-select basic-mgmt

Use this command to select basic management TLVs to be include in the LLDP frames.

Use the no parameter to disable basic management TLVs.

Command Syntax

```
lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
no lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`
: Management address specific TLV

`port-description`
: Port description specific TLV

`system-capabilities`
: System capabilities specific TLV

`system-description`
: System Description specific TLV

`system-name`
: System name specific TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select basic-mgmt system-name
```

lldp tlv-select ieee-8021-org-specific

Use this command to select ieee-8021-org-specific TLVs to include in the LLDP frames.

Use the no parameter to disable ieee-8021-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-vlanid|ptcl-identity|vid-digest|vlan-name)
no lldp tlv-select ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-identity| vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8021-org-specific port-vlanid
```

lldp tlv-select ieee-8023-org-specific

Use this command to select ieee-8023-org-specific TLVs to be include in LLDP frames.

Use the no parameter to disable ieee-8023-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
no lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	VLAN ID Of the provider edge port <2-4094>.
`power-via-mdi`	Power-via-MDI (only when PoE feature is available)
`max-mtu-size`	Maximum MTU size TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8023-org-specific mac-phy
```

set lldp agt-circuit-id

Use this command to configure LLDP agt-circuit-id.

Command Syntax

```
set lldp agt-circuit-id  VALUE
```

Parameters

VALUE	Specify LLDP global agt-circuit ID.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#set lldp agt-circuit-id sample
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Use no form of this command to unset the chassis ID subtype.

Command Syntax

```
set lldp chassis-id-tlv (if-alias | ip-address | mac-address | if-name | locally-
  assigned)
no set lldp chassis-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID
`if-alias`	Use the IP address as the chassis ID
`if-name`	Use the interface name as the chassis ID
`locally-assigned`	Use the locally assigned value as the chassis ID

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp chassis-id-tlv ip-address
(if-lldp-agent)#no set lldp chassis-id-tlv
```

set lldp chassis locally-assigned

Use this command to set the locally assigned chassis name for the LLDP interface.

Command Syntax

```
set lldp chassis locally-assigned NAME
```

Parameters

NAME	Name assigned to the chassis.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#set lldp chassis locally-assigned box1
```

set lldp disable

Use this command to disable the admin status of a LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp disable
(if-lldp-agent)#exit
```

set lldp enable

Use this command to set the admin status of a LLDP agent on a port.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp enable txrx
(if-lldp-agent)#exit
```

set lldp locally-assigned

Use this command to set the locally assigned name for LLDP interface.

Use no form of this command to remove the locally assigned name for LLDP interface.

Command Syntax

```
set lldp locally-assigned NAME
no set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp locally-assigned port1
(config-if)#no set lldp locally-assigned
```

set lldp management-address-tlv

Use this command to set the sub type of the Management Address TLV.

Use no form of this command to unset the sub type of the Management Address TLV.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
no set lldp management-address-tlv
```

Parameters

mac-address	Use the MAC address as the Management Address.
ip-address	Use the management IP address as the Management Address.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp management-address-tlv ip-address
(if-lldp-agent)#no set lldp management-address-tlv
```

set lldp med-devtype

Use this command to configure the LLDP device type as Network-Connectivity/ End-Point Class1/ End-Point Class2/ End-Point Class3 device.

Use the no parameter to un set the configured LLDP device type.

Command Syntax

```
set lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
no lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
```

Parameters

`net-connect`	Set device type as Network-Connectivity
`ep-class1`	Set device type as End-Point Class1
`ep-class2`	Set device type as End-Point Class2
`ep-class3`	Set device type as End-Point Class3

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp med-devtype ep-class1
(config-if)#exit

#configure terminal
(config)#interface eth0
(config-if)#no set lldp med-devtype
(config-if)#exit
```

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer` `msg-tx-interval` value, which determines the final TTL value.

Use `no` form of this command to set the default value of message transmit hold.

Command Syntax

```
set lldp msg-tx-hold <1-100>
no set lldp msg-tx-hold
```

Parameters

`<1-100>`	Time in seconds to set message transmit hold.

Default

The default value of message transmit hold is 4 seconds.

Command Mode

LLDP agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp msg-tx-hold 3
(if-lldp-agent)#no set lldp msg-tx-hold
```

set lldp port-id-tlv

Use this command to set the sub type of the Port ID.

Use no form of this command to unset the sub type of the Port ID.

Command Syntax

```
set lldp port-id-tlv (if-alias | ip-address | mac-address | if-name | agt-circuit-
  id | locally-assigned)
no set lldp port-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the port-id-tlv.
`ip-address`	Use the management IP address as the port-id-tlv
`if-alias`	Use the IP alias as the port-id-tlv
`if-name`	Use the interface name as the port-id-tlv
`agt-circuit-id`	Use the agt-circuit-id name as the port-id-tlv
`locally-assigned`	Use the locally assigned value as the port-id-tlv

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp port-id-tlv ip-address
(if-lldp-agent)#no set lldp port-id-tlv
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Use no form of this command to set the default value for timer.

Command Syntax

```
set lldp timer msg-fast-tx <1-3600>
set lldp timer msg-tx-interval <5-3600>
set lldp timer reinit-delay <1-10>
no set lldp timer msg-fast-tx
no set lldp timer msg-tx-interval
no set lldp timer reinit-Delay
```

Parameters

`msg-fast-tx`	Set the value in range <1-3600>
`msg-tx-interval`	Set the value in range <5-3600>
`reinit-delay`	Set the value in range <1-10>

Default Values

The default value for `msg-fast-tx` is 1 second.

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinit-delay` is 2 seconds.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-fast-tx 40
(if-lldp-agent)#no set lldp timer msg-fast-tx
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-tx-interval 40
(if-lldp-agent)#no set lldp timer msg-tx-interval
(if-lldp-agent)#exit
```

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer reinitDelay 3
(if-lldp-agent)#no set lldp timer reinitDelay
(if-lldp-agent)#exit
```

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Use no form of this command to unset too many neighbors parameters.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC timer <1-
  65535>
no set lldp too-many-neighbors limit
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	Upper limit for the number of Remote LLDP Information.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 20 disc existing-info
1001.1001.1001 timer 1

(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 1 discard received-info
timer 1
```

set lldp tx-fast-init

Use this command to determine the maximum value of LLDP frames that are transmitted during a fast transmission period.

Use no form of this command to set fast transmission period to default value.

Command Syntax

```
set lldp tx-fast-init <1-8>
no set lldp tx-fast-init
```

Parameters

tx-fast-init	Set the message transmit interval value <1-8>.

Default Value

Default value is 4.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp tx-fast-init 4
(if-lldp-agent)#no set lldp tx-fast-init
(if-lldp-agent)#exit
```

set lldp tx-max-credit

Use this command to set the maximum value of transmission credit, which signifies the number of consecutive LLDP frames transmitted.

Use no form of this command to set the maximum value of transmission credit to default value.

Command Syntax

```
set lldp tx-max-credit <1-10>
no set lldp tx-max-credit
```

Parameters

tx-max-credit	The maximum value of transmission credit.

Default Value

Default value is 5

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#set lldp tx-max-credit <1-10>
(if-lldp-agent)#no set lldp tx-max-credit
(if-lldp-agent)#exit
```

show debugging lldp

Use this command to display LLDP debugging information.

Command Syntax

```
show debugging lldp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sample output displays information about an LLDP debugging.

```
#show debugging lldp
LLDP debugging status:
 LLDP message debugging is on
```

show lldp neighbors

Use this command to display LLDP neighbors information.

Command Syntax

```
show lldp (nearest-bridge| non-tpmr-bridge| customer-bridge|) neighbors
  (brief|details)
```

Parameters

nearest-bridge	Display LLDP nearest bridge information
non-tpmr-bridge	Display LLDP non-TPMR-bridge information
customer-bridge	Display LLDP customer-bridge information
neighbor	Neighbor
brief	Brief
details	Details

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.1.

Example

The following sample output displays information about an LLDP neighbors

```
#sh lldp nearest-bridgr neighbors brief
Loc PortID  Rem Host Name   Rem Chassis Id  Rem Port Id   Agent Mode

-------------------------------------------------------------------------------
xe3/1        OcNOS       ecf4.bbfe.2864  ecf4.bbb2.4c65 Nearest bridge


#show lldp neighbors detail

-------------------------------------------------------------------------------
Nearest bridge Neighbors
 Interface Name : xe11
 Mandatory TLVs
 Chassis id type : MAC address [8cea.1b67.236c]
 Port id type : MAC address [8cea.1b28.4f6d]
 Time to live : 121
 Basic Management TLVs
 System Name : OcNOS
 System Description : Hardware Model:EC_AS5912-54X, Software version: OcNOS,1.3.1.122
 Port Description : xe11
 Remote System Capabilities : Bridge Router
 Capabilities Enabled : Router
```

```
Management Address : MAC Address [8cea.1b67.236c]
Interface Number subtype : ifindex
Interface Number : 10011
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID :
802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode only]
Max Frame Size : 1518
```

Table 1-51 Shows the output details.

Table 1-50: show lldp neighbor output details

Entry	Description
Loc Port ID	Local interface SNMP index (appears when the interface option is used).
Rem Host Name	Name of the remote host.
Rem Chassis Id	Remote chassis identifier of the chassis type listed.
Rem Port Id	Remote port identifier of the port type listed.
Agent Mode	Agent mode enabled to the nearest bridge.
Time to live	Number of seconds for which this information is valid.
Interface Name	Name of the interface.
Chassis id type	Chassis identifier of the chassis type listed.
Port id type	Type of port identifier supplied, such as Locally assigned.
System Name	Name supplied by the system on the interface.
System Description	Description supplied by the system on the interface.
Port Description	The port description field uses the configured port description, the port name or the SNMP if Index (appears when the interface option is used).
Remote System Capabilities	Remote system capabilities (such as Bridge, Bridge Router, and Bridge Telephone) that are supported.

Table 1-50: show lldp neighbor output details

Entry	Description
Capabilities Enabled	Enabled by the system on the interface (appears when the interface option is used).
Management Address	Details of management address (such as 10.204.35.34).
Interface Number subtype	Interfaces subtype for which neighbor information is available.
Interface Number	Interfaces for which neighbor information is available.
OID Number	Number of identifier.
Port VLAN ID	Details of the port VLAN identifier.
Protocol VLAN ID	Details of the protocol VLAN identifier.
Remote Configured VLANs	Details of the remote configured VLAN.
Remote Protocols Advertised	Details of the remote protocols.
Remote VID usage Digest	Details of the VID usage.
Remote Management VLAN	Details of the management VLAN.
Link Aggregation Capability	Capabilities that supported by the link aggregation on the interface.
Link Aggregation Status	Status of the link aggregation.
Link Aggregation Port ID	Details of the link aggregation port identifier.
Auto Nego Support	Support of the auto nego on the interface.
Auto Nego Status	Status of the auto nego.
Auto Nego Capability	Capabilities that supported by the auto nego on the interface.
Operational MAU Type	Type of operational MAU on the interface.
Max Frame Size	Maximum frame size on the transit.

show lldp interface

Use this command to display LLDP interface information.

Command Syntax

```
show lldp interface IFNAME (nearest-bridge| non-tpmr-bridge| customer-bridge | )
  (neighbor| )
```

Parameters

`IFNAME`

Display LLDP interface information for all agent

`nearest-bridge`

Display LLDP nearest bridge information

`non-TPMR-bridge`

Display LLDP non-TPMR-bridge information

`customer-bridge`

Display LLDP customer-bridge information

`neighbor`

Display LLDP neighbor details.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lldp interface eth0
Agent Mode : Customer-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Non-TPMR-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
```



```
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 2495
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

Table 1-51 Shows the output details.

Table 1-51: show lldp interface output details

Entry	Description
Agent Mode	Agent mode enabled to the customer-bridge, Non-TPMR-bridge, and nearest bridge.
Enable (tx/rx)	Enables the transmit and receive on the interface.
Device Type	Type of device in the networks.
LLDP Agent traffic statistics	Statistics on exchanged LLDP frames between a device and neighbors.
Total frames transmitted	Number of frames transmitted in network.
Total entries aged	Number of aged entries in a networks.
Total frames received	Number of frames received from the neighbor network.
Total frames received in error	Number of frames not received from the neighbor network.
Total discarded TLVs	Number of TLVs discarded in transit.
Total unrecognised TLVs	Number of unrecognised TLVs in transit.

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lldp
```

CHAPTER 2 Provider Bridging Commands

This chapter describes the Provider Bridging (PB) commands.

IEEE 802.1ad standardizes the architecture and bridged protocols to allow Ethernet frames with multiple VLAN tags. Packets through a provider network are doubly tagged with both an:

- Inner (C-VLAN) tag which is the customer network VLAN identifier
- Outer (S-VLAN) tag which is the service provider network VLAN identifier

bridge protocol provider-rstp

Use this command to add an IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Command Syntax

```
bridge <1-32> protocol provider-rstp (edge|)
```

Parameters

`<1-32>`	Bridge identifier.
`edge`	Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-rstp edge
```

clear l2protocol interface counters

This command allows you to clear the counters for numbers of packets peered, discarded and tunneled.

Command Syntax

```
clear l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

`peer`	Clear stats for Peer protocol packets.
`discard`	Clear stats for Tunnel protocol packets.
`tunnel`	Clear stats for Tunnel protocol packets.
`tunnel-discard`	Clear stats for Tunnel discard protocol packets.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
# clear l2protocol interface xe1 counters peer
```

cvlan registration table

Use this command to create a customer VLAN (CVLAN) registration table that maps between CVLANs and service provider VLANs (SVLANs).

Use the no parameter with this command to delete the CVLAN registration table.

Command Syntax

```
cvlan registration table WORD bridge <1-32>
no cvlan registration table WORD bridge <1-32>
```

Parameters

WORD	Name of the CVLAN registration table.
<1-32>	Specify a bridge ID.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#cvlan registration table customer1
(config-cvlan-registration)#
```

cvlan svlan

Use this command to map one or more customer VLANs (CVLANs) to a service provider VLAN (SVLAN).

To update the optional QoS parameters cos-to-queue and remark-cos, execute the complete command along with the optional parameters. To remove these options, execute the same command by removing the optional parameters.

Refer qos profile commands from configuration guide for more details about qos profiles.

Use the no forms of this command to delete a mapping.

Command Syntax

```
cvlan VLAN_RANGE2 (cvlan VLAN_ID|) svlan VLAN_ID ({cos-to-queue NAME | remark-
  cos}|)
no cvlan VLAN_RANGE2
no svlan VLAN_ID
```

Parameters

`cvlan`	CVLAN
`VLAN_RANGE2`	VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19
`cvlan`	Translation of CVID
`VLAN_ID`	Translated CVID <1-4095>
`svlan`	SVLAN corresponding to the C-VLAN
`VLAN_ID`	VLAN identifier 1-4094>
`cos-to-queue`	Configure cos-to-queue map for cvlan
`NAME`	Ingress profile to modify queue/color on basis of c-cos
`remark-cos`	Remark Egress COS

Command Mode

CVLAN Registration mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#cvlan registration table customer1 (config-cvlan-registration)#cvlan
2 svlan 3
(config-cvlan-registration)#cvlan 3 svlan 3 cos-to-queue c1 remark-cos
(config-cvlan-registration)#cvlan 100 cvlan 101 svlan 200 cos-to-queue p1
remark-cos
(config-cvlan-registration)#cvlan 3 svlan 3 remark-cos
(config-cvlan-registration)#no cvlan 3
```

l2protocol

This command allows you to change the process of protocol to peer/discard/tunnel.

Command Syntax

```
l2protocol (stp|lacp|efm|elmi|lldp|synce)(peer|discard|tunnel)
```

Parameters

`stp`	Spanning Tree Protocols.
`lacp`	Link Aggregation (LACP).
`efm`	Ethernet first mile (Link OAM).
`elmi`	Ethernet local management interface.
`lldp`	Link layer discovery protocol.
`synce`	Link layer discovery protocol.
`peer`	Act as peer to the customer Device instance of the protocol.
`discard`	Discard the protocol data unit.
`tunnel`	Tunnel the Protocol data unit into the SVLAN.

Default

Default process value is peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge access
(config-if)#l2protocol stp tunnel
(config-if)#l2protocol stp peer
(config-if)#l2protocol stp discard
```

l2protocol encapsulation dest-mac

Use this command to change destination mac of tunneled l2 protocol packet. Allowed mac are 0100.C2CD.CDD0 or 0104.DFCD.CDD0.

Use the no parameter with this command to set default mac 0100.C2CD.CDD0.

Command Syntax

```
bridge <1-32> l2protocol encapsulation dest-mac XXXX.XXXX.XXXX
no bridge <1-32> l2protocol encapsulation dest-mac
```

Parameters

bridge	Bridge group for bridging.
<1-32>	<1-32>
l2protocol	Configure Layer2 Protocol Tunneling.
encapsulation	Encapsulation of L2PT packet.
dest-mac	Encapsulation with destination mac.
XXXX.XXXX.XXXX	Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or 0104.DFCD.CDD0).

Command Mode

Configuration mode

Applicability

This command is introduced in OcNOS-SP version 1.0.

Examples

```
(config)#bridge 1 l2protocol encapsulation dest-mac ?
XXXX.XXXX.XXXX Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or
0104.DFCD.CDD0)
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#

(config)#no bridge 1 l2protocol encapsulation dest-mac
(config)#show running-config | in bridge
bridge 1 protocol provider-rstp edge
vlan 2-10 type customer bridge 1 state enable
vlan 11-12 type service point-point bridge 1 state enable
cvlan registration table map1 bridge 1
bridge-group 1
bridge-group 1
(config)#
```

show cvlan registration table

Use this command to display the CVLAN registration table.

Command Syntax

```
show cvlan registration table (WORD|bridge <1-32>|WORD bridge <1-32>|)
```

Parameters

WORD	CVLAN registration table name.
<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh cvlan registration table bridge 1
Bridge          Table Name       Port List
======          ==========       =========
  1               map              xe17

CVLAN ID      T-CVLAN ID     SVLAN ID     Profile Name    Egress remark-Cos
 ========    ==========     ========    ============    =================
 100             101            200          p1              Yes
```

Table 2-52 explains the output fields.

Table 2-52: show cvlan registration table output

Entry	Description
Bridge	ID number of the bridge associated with the Customer VLAN (CVLAN).
Table Name	ID of the CVLAN registration table.
Port List	List of ports used by this CVLAN (including Link aggregators).
CVLAN ID	ID number of the CVLAN.
T-CVLAN ID	Translation CVLAN ID.
SVLAN ID	ID number of the Service VLAN (SVLAN) associated with the CVLAN.
Profile Name	cos-to-queue profile name.
Egress remark-Cos	Remark Egress Cos

show l2protocol interface counters

This command allows you to display the counters for numbers of packets peered, discarded and tunneled.

Command Syntax

```
show l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

`peer`	Display stats for Peer protocol packets.
`discard`	Display stats for Tunnel protocol packets.
`tunnel`	Display stats for Tunnel protocol packets.
`tunnel-discard`	Display stats for Tunnel discard protocol packets.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
# show l2protocol interface xe1 counters peer
Interface xe1
Peer:     stp:    1

# show l2protocol interface xe1 counters
Interface xe1
Peer:     stp:    1
Discard:  stp:    10
Tunnel:   stp:    5
```

show l2protocol processing interface

This command allows you to display the processing information on Layer 2 protocol interface.

Command Syntax

```
show l2protocol processing interface IFNAME
```

Parameters

IFNAME	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command is introduced was before OcNOS-SP version 1.0.

Examples

```
#show l2protocol processing interface xe1/1
Bridge    Interface Name                Protocol       Processing Status
======    ==============                ========       =================
1         xe1/1                          stp            Tunnel
1         xe1/1                          gmrp           Peer
1         xe1/1                          gvrp           Peer
1         xe1/1                          mmrp           Peer
1         xe1/1                          mvrp           Peer
1         xe1/1                          lacp           Peer
1         xe1/1                          lldp           Peer
1         xe1/1                          efm            Peer
1         xe1/1                          elmi           Peer
1         xe1/1                          ptp            Peer
1         xe1/1                          synce          Peer
```

switchport customer-edge

Use this command to set the switching characteristics of the layer 2 interface and the default customer VLAN.

Use the no form of this command to remove a customer VLAN.

Command Syntax

```
switchport customer-edge (access|hybrid) vlan <2-4094>
no switchport customer-edge (access|hybrid) vlan
```

Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`<2-4094>`	Set the default VID for the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-edge access vlan 3

(config)#interface eth0
(config-if)#no switchport customer-edge access vlan
```

switchport customer-edge hybrid

Use this command to set the switching characteristics of the Layer 2 customer-facing interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Command Syntax

```
switchport customer-edge hybrid allowed vlan add VLAN_ID
switchport customer-edge hybrid allowed vlan remove VLAN_ID
switchport customer-edge hybrid allowed vlan all
switchport customer-edge hybrid allowed vlan none
```

Parameters

`add`	Add a VLAN to transmit and receive through the Layer 2 interface.
`VLAN_ID`	ID of the VLAN <2-4094>.
`remove`	Remove a VLAN from the member set.
`VLAN_ID`	ID of the VLAN <2-4094>.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport customer-edge hybrid allowed vlan add 2
```

switchport customer-edge trunk

Use this command to set the Layer2 interface as trunk.

Command Syntax

```
switchport customer-edge trunk allowed vlan add VLAN_ID
switchport customer-edge trunk allowed vlan remove VLAN_ID
switchport customer-edge trunk allowed vlan all
switchport customer-edge trunk allowed vlan none
```

Parameters

`add`	Add a VLAN to the member set.
`VLAN_ID`	Specify a VLAN ID <2-4094>
`remove`	Remove a VLAN from the member set.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge trunk allowed vlan add 12
```

switchport customer-edge vlan registration

Use this command to configure the VLAN registration parameters.

Use the no parameter with this command to delete the mapping from the interface.

Command Syntax

```
switchport customer-edge vlan registration WORD
no switchport customer-edge vlan registration
```

Parameters

WORD	Name of the CVLAN registration table.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge vlan registration customer1
```

switchport dot1q

This command allows you to change the TPID for a port.

Use the no form of this command to unset the TPID to default value.

Command Syntax

```
switchport dot1q ethertype ETHERTYPE
no switchport dot1q ethertype
```

Parameters

dot1q	Set the switching characteristics of the Layer2 dot1q header.
ETHERTYPE	Ethertype value for outer tag (Allowed ethertype values are 0x8100 (default) or 0x88a8 0r 0x9100 or 0x9200)

Default

The default TPID value is 8100.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)# switchport dot1q ethertype 0x88a8
(config-if)# no switchport dot1q ethertype
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Command Syntax

```
switchport mode (provider-network|customer-edge)
```

Parameters

`provider-network` Provider network.

`customer-edge` Customer edge.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network
```

switchport mode customer-edge

Use this command to set the switching characteristics of the Layer 2 customer facing interface and classify only untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode customer-edge (access|hybrid|trunk)
```


```
switchport mode customer-edge (access|hybrid|trunk)
```


Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`trunk`	Set the layer 2 interface as trunk.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge access
```

switchport provider-network isolated-vlan

Use this command to attach a VLAN as an isolated VLAN for a provider network port.

Using an isolated VLAN for PNP ports on a switch can forward all frames received from the PNP port to all other PNP ports. However, if VLANs are configured to be isolated, they can traverse PNP port without sharing any of their frames.

Use the no form of this command to remove an isolated VLAN for a provider network port.

Command Syntax

```
switchport provider-network isolated-vlan VLAN_RANGE
no switchport provider-network isolated-vlan VLAN_RANGE
```

Parameters

VLAN_RANGE	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#bridge 1 protocol provider-rstp
(config)#vlan database
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable
(config-vlan)#exit
(config)#interface xe0
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport provider-network allowed vlan all
(config-if)#switchport provider-network isolated-vlan 2-10
```

vlan type customer

Use this command to configure VLANs of type customer, to enable or disable the state of the VLANs, and to configure the name for VLANs.

Use the no form of this command to remove the VLAN type.

Command Syntax

```
vlan <2-4094> type customer bridge <1-32>
vlan <2-4094> type customer bridge <1-32> state (enable|disable)
vlan <2-4094> type customer bridge <1-32> name WORD
no vlan <2-4094> type customer bridge <1-32>
```

Parameters

<2-4094>	The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.
type	Identifies the VLAN as a customer, service, or VLAN.
customer	Identifies the Customer VLAN
bridge	Indicates a Service VLAN <1-32>.
name	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state.
WORD	ASCII name of the VLAN.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 12 type customer bridge 1 name new state enable
```

vlan type

This command allows you to create a single/range of VLAN's on provide/edge bridge.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type customer bridge <1-32>
vlan VLAN_RANGE type customer bridge <1-32> name WORD
vlan VLAN_RANGE type customer bridge <1-32> state (enable | disable)
vlan VLAN_RANGE type service point-point bridge <1-32>
vlan VLAN_RANGE type service point-point bridge <1-32> name WORD
vlan VLAN_RANGE type service point-point bridge <1-32> state (enable | disable)

no vlan VLAN_RANGE type customer bridge <1-32>
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

VLAN_RANGE	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19
customer	Identifies the Customer VLAN
bridge	Specify the bridge group ID in the range <1-32>.
name	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
point-point	Sets the VLAN connectivity mode to point-to-point
WORD	ASCII name of the VLAN.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)vlan 2,4,5-6 customer bridge 2
(config)vlan 10-12 service type point-point bridge 3
```

CHAPTER 3 CFM and Y.1731 Commands

This chapter describes the commands used to manage the Connectivity Fault Management (CFM). CFM refers to the service OAM of Ethernet used to manage individual Layer 2 Ethernet services. The CFM protocol can discover and verify the path through 802.1 bridges and LANs. OcNOS adheres to the IEEE 802.1ag 2007 standard.

CFM includes the features required by ITU Y.1731 standard *OAM Functions and Mechanisms for Ethernet Based Networks*. This recommendation identifies the functions required to enable fault management (such as fault localization and defect detection) and performance monitoring in an Ethernet network.

- mep crosscheck
- mep lowest-priority-defect
- message-period
- number-intervals-stored
- ping ethernet mac
- rmep auto-discovery
- service ma-type
- show ethernet cfm ais reception-status
- show ethernet cfm delay-measurement mep
- show ethernet cfm delay-measurement profile
- show ethernet cfm dm sessions
- show ethernet cfm errors
- show ethernet cfm frame-lm session
- show ethernet cfm loss-measurement mep
- show ethernet cfm loss-measurement profile
- show ethernet cfm ma status
- show ethernet cfm maintenance-points local mep
- show ethernet cfm maintenance-points local mip
- show ethernet cfm maintenance-points remote
- show ethernet cfm statistics
- show running-config cfm
- traceroute ethernet
- ethernet cfm test-signal profile-name
- test-signal mode
- test-signal test-type
- test-signal frame-size
- test-signal pattern-type
- test-signal start-time
- abort test-signal domain
- show ethernet cfm test-signal profile
- show ethernet cfm test-signal domain
- eth-lck state
- eth-lck message
- eth-lck interval
- eth-lck frame priority
- show ethernet cfm lck statistics
- show ethernet cfm lck details domain

abort delay-measurement

Use this command to stop the ongoing or scheduled CFM frame delay measurement session.

Command Syntax

```
abort delay-measurement mep MEPID domain DOMAIN_NAME (vlan <2-4094>|bridge <1-
  32>|vpws)
```

Parameters

MEPID	MEP identifier <1-8191>
DOMAIN_NAME	MD name
<2-4094>	VLAN identifier
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#abort delay-measurement mep 123 domain 12345 vlan 10 bridge 1
#abort delay-measurement mep 123 domain 12345 vpws
```

abort loss-measurement

Use this command to stop the ongoing CFM frame loss measurement session.

Command Syntax

```
abort loss-measurement mep MEPID domain DOMAIN_NAME (vlan <2-4094>|bridge <1-
  32>|vpws)
```

Parameters

MEPID	MEP identifier <1-8191>
DOMAIN_NAME	MD name
<2-4094>	VLAN identifier
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#abort loss-measurement mep 201 domain 12345 vlan 10 bridge 1
#abort loss-measurement mep 201 domain 12345 vpws
```

ais interval

Use this command to set the AIS (Alarm Indication Signal) transmission interval.

Command Syntax

```
ais interval (one-second | one-minute)
```

Parameters

`one-second`	AIS transmission interval in packets per second
`one-minute`	AIS transmission interval in packets per minute

Default

`one-second`

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#ais interval one-minute
```

ais status

Use this command to enable or disable AIS (Alarm Indication Signal) transmission and set the CFM MD level to transmit in AIS PDUs.

Command Syntax

```
ais status (enable|disable) level <0-7>
```

Parameters

`enable`	Enable AIS
`disable`	Disable AIS
`<0-7>`	CFM MD level

Default

`disable`

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#ais status enable level 7
```

bins-per-fd-interval

Use this command to the set number of measurement bins per measurement interval for a two-way performance monitoring frame delay measurements on a specific MEP.

Use the no form to set number of measurement bins per measurement interval for a two-way performance monitoring frame delay measurements on a specific MEP to its default (3).

Command Syntax

```
bins-per-fd-interval <2-10>
no bins-per-fd-interval
```

Parameters

<2-10>	Number of frame delay bins to be created

Default

3

Command Mode

Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)# bins-per-fd-interval 4
```

bins-per-ifdv-interval

Use this command to set the number of measurement bins per measurement interval for an inter-frame delay for a two-way performance monitoring frame delay measurements on a specific MEP.

Use the no form to set the number of measurement bins per measurement interval for an inter-frmae delay for a two-way performance monitoring frame delay measurements on a specific MEP to its default (2).

Command Syntax

```
bins-per-ifdv-interval <2-10>
no bins-per-ifdv-interval
```

Parameters

<2-10>	Number of inter-frame delay bins to be created

Default

2

Command Mode

Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)# bins-per-ifdv-interval 3
```

bin-type

Use this command to set the threshold value for a particular bin for a two-way performance monitoring frame delay measurements on a specific MEP.

Use the no form to set threshold value for a particular bin for a two-way performance monitoring frame delay measurements on a specific MEP to its default.

Command Syntax

```
bin-type frame-delay bin 2 threshold 200
no bin-type frame-delay bin 2 threshold
bin-type inter-frame-delay-variation bin 2 threshold 1000
no bin-type inter-frame-delay-variation bin 2 threshold
```

Parameters

`frame-delay`	Frame delay bin type
`inter-frame-delay-variation`	Inter frame delay variation bin type
`<2-10>`	Bin number for which the threshold will be changed.
`<1- 4294967295>`	Threshold value for that bin.

Default

Incremental of 5000 microseconds from bin 2, that is bin 2's threshold will be 5000, bin 3's will be 10000, bin 4 will be 15000, so on and so forth.

Command Mode

Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)# bin-type frame-delay bin 2 threshold 200
(config-cfm-dm)# bin-type inter-frame-delay-variation bin 2 threshold 1000
```

cc interval

Use this command to set the continuity checking (CC) message interval.

Command Syntax

```
cc interval (1|2|3|4|5)
```

Parameters

1	3 milliseconds
2	10 milliseconds
3	100 milliseconds
4	1 seconds
5	10 seconds

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#cc interval 1
```

cc multicast

Use this command to start or stop multicast continuity checking messages (CCMs) on a MEP.

Command Syntax

```
cc multicast state (enable|disable)
```

Parameters

`enable`	Start sending CCMs
`disable`	Stop sending CCMs

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#cc multicast state enable
```

clear ethernet cfm dm history

Use this command to clear the CFM frame delay measurement history statistics from CFM_MEP DB.

Command Syntax

```
clear ethernet cfm dm history mep MEPID domain DOMAIN_NAME (vlan <2-4094>| bridge
  <1-32> | vpws VCNAME)
```

Parameters

MEPID	Local MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
<2-4094>	Primary VLAN identifier of MA.
<1-32>	Bridge identifier
VCNAME	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm dm history mep 123 domain no_name vlan 10 bridge 1
```

clear ethernet cfm lm history

Use this command to clear the CFM frame loss measurement history statistics.

Command Syntax

```
clear ethernet cfm lm history mep MEPID domain DOMAIN_NAME (vlan <2-4094>|bridge
  <1-32>|vpws VCNAME)
```

Parameters

MEPID	Local MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
<2-4094>	Primary VLAN identifier of MA.
<1-32>	Bridge identifier
VCNAME	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm lm history mep 201 domain 12345 vlan 10 bridge 1
#clear ethernet cfm lm history mep 201 domain 12345 vpws
```

clear ethernet cfm maintenance-point remote

Use this command to remove a dynamically learned RMEP.

The RMEP is relearned if rmep auto-discovery is enabled and a CCM (Continuity Checking Message) is received.

Command Syntax

```
clear ethernet cfm maintenance-points remote (domain <DOMAIN_NAME>|level <0-7>)
  (bridge <1-32> | vpws)
```

Parameters

DOMAIN_NAME	MD name
<0-7>	CFM level
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm maintenance-point level 7 bridge 1
#clear ethernet cfm maintenance-point level 6 vpws
```

clear ethernet cfm statistics

Use this command to clear the CFM statistics.

Command Syntax

```
clear ethernet cfm statistics mep <MEPID> domain <DOMAIN_NAME> (vlan <2-4094>
  bridge <1-32>)
```

Parameters

MEPID	MEP identifier <1-8191>
DOMAIN_NAME	MD name
<2-4094>	Primary VLAN identifier
<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm statistics mep 201 domain 12345 vlan 10 bridge 1
```

clear ethernet cfm traceroute-cache

Use this command to clear the CFM traceroute cache entry.

Command Syntax

```
clear ethernet cfm traceroute-cache (bridge <1-32>|vpws)
```

Parameters

<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm traceroute-cache bridge 1
#clear ethernet cfm traceroute-cache vpws
```

delay-measurement type on-demand

Use this command to schedule an on-demand CFM delay measurement session.

Command Syntax

```
delay-measurement type on-demand profile-name WORD rmep (mac-address MAC|RMEPID)
  start-time (immediate|relative HH:MM:SS|absolute HH:MM:SS <1-31> MONTH <1993-
  2035>) repetition-period <6000-4294967295> mep MEPID domain DOMAIN_NAME (vlan <2-
  4094>| bridge <1-32> | vpws VCNAME)
```

Parameters

`WORD`	Delay measurement profile name
`MAC`	Destination MAC address in HHHH.HHHH.HHHH format
`RMEPID`	Destination peer MEP identifier <1-8191>
`start-time`	Measurement session start time
`immediate`	Start immediately
`relative HH:MM:SS`	Relative time to start from the current system time
`absolute HH:MM:SS <1-31> MONTH <1993-2035>`	Scheduled date and time to start; for the month, specify the first three letters
`stop-time`	Measurement session stop time
`none`	Never stop
`relative HH:MM:SS`	Relative time to stop from the current system time
`absolute HH:MM:SS <1-31> MONTH <1993-2035>`	Scheduled date and time to stop; for the month, specify the first three letters
`<6000-4294967295>`	Repetition time in centiseconds
`MEPID`	Local MEP identifier <1-8191>
`DOMAIN_NAME`	Maintenance domain name
`<2-4094>`	Primary VLAN identifier of the MA
`<1-32>`	Bridge identifier
`VCNAME`	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#delay-measurement type on-demand profile-name PROF1 rmep 101 start-time relative
00:00:03 stop-time relative 00:03:00 repetition-period 7000 mep 123 domain no_name vlan
10 bridge 1
```

delay-measurement type proactive

Use this command to configure and start a proactive CFM delay measurement session.

Command Syntax

```
delay-measurement type proactive profile-name WORD rmep (mac-address MAC|RMEPID)
  mep MEPID domain DOMAIN_NAME (vlan <2-4094>| bridge <1-32> | vpws VCNAME)
```

Parameters

WORD	Delay measurement profile name
MAC	Destination MAC address in HHHH.HHHH.HHHH format
RMEPID	Remote MEP identifier <1-8191>
MEPID	Local MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
<2-4094>	Primary VLAN identifier of the MA
<1-32>	Bridge identifier
VCNAME	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#delay-measurement type proactive profile-name 123 rmep 101 mep 123 domain no_name vlan
10 bridge 1
#delay-measurement type proactive profile-name 123 rmep 101 mep 123 domain no_name vpws
ETH-2001
```

ethernet cfm delay-measurement profile-name

Use this command to create a CFM frame delay measurement profile and enter Ethernet CFM delay measurement mode.

Use the no form of this command to remove a CFM delay measurement profile.

Command Syntax

```
ethernet cfm delay-measurement profile-name WORD
no ethernet cfm delay-measurement profile-name WORD
```

Parameters

WORD	Profile name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)#
```

ethernet cfm delay-measurement reply

Use this command to enable transmission of DMR (Delay Measurement Reply) PDUs for received DMMs (Delay Measurement Messages).

After this command is given, a delay measurement session cannot be configured to send DMMs. In that case, the device can only generate DMRs for received DMM PDUs.

Use the no form of this command to disable sending DMR PDUs. After no command is given we can thereby configure a delay measurement session to send DMMs if we need.

Command Syntax

```
ethernet cfm delay-measurement reply dmm
```

```
no ethernet cfm delay-measurement reply dmm
```

Parameters

None

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)# ethernet cfm domain-type no-name domain-name no_name level 4 mip-creation none
bridge 1
(config-ether-cfm)# service ma-type integer ma-name 200 vlan 10 mip-creation none
(config-ether-cfm-ma)# ethernet cfm mep down mpid 123 active true local-vid 10 xe1
(config-ether-cfm-ma-mep)#ethernet cfm delay-measurement reply dmm
```

ethernet cfm domain-type

Use this command to create a CFM Maintenance Domain (MD) in a bridge and enter Ethernet CFM mode.

Use the no form of this command to remove a domain.

Note: You can create up to 15 MDs in a bridge.

Only one domain can be created without any domain name in a bridge.

A domain name of type `character-string` can only created only after the hardware-profile filter cfm-domain-name-str command is executed.

Command Syntax

```
ethernet cfm domain-type (no-name|character-string) domain-name DOMAIN_NAME level
  <0-7> mip-creation (none|default|explicit) (bridge <1-32> | vpws)
no ethernet cfm domain-name DOMAIN_NAME level <0-7> mip-creation
  (none|default|explicit) (bridge <1-32> | vpws)
```

Parameters

`domain-type`	Domain type (must match service ma-type setting)
`no-name`	No MD name. The `ma-type` must be `integer` or `itu-t` carrier code (ICC) format defined by Y.1731.
`character-string`	Character string name. The `ma-type` must be string.
`DOMAIN_NAME`	Domain name (name must be a 5-character string)
`<0-7>`	MD level
`mip-creation`	Maintenance Intermediate Point (MIP) creation permission for this domain
`none`	No MIP can be created for this VLAN identifier
`default`	MIP can be created if no lower active level or MEP at next lower active level
`explicit`	Maintenance End Point (MEP) is needed at the next lower active level
`<1-32>`	Bridge identifier
`vpws`	VPWS instance

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe7
```

```
(config-ether-cfm-ma-mep)#
```

ethernet cfm loss-measurement profile-name

Use this command to create a CFM frame loss measurement profile and enter Ethernet CFM loss measurement mode.

Use the no form of this command to remove a CFM loss measurement profile.

Command Syntax

```
ethernet cfm loss-measurement profile-name WORD
no ethernet cfm loss-measurement profile-name WORD
```

Parameters

WORD	Profile name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm loss-measurement profile-name PROF1
(config-cfm-lm)#
```

ethernet cfm loss-measurement reply

Use this command to enable transmission of SLR (Synthetic Loss Reply) PDUs for received SLMs (Synthetic Loss Messages) and to enable transmission of LMR (Loss Measurement Reply) PDUs for received LMMs (Loss Measurement Messages).

After this command is given, a loss measurement session cannot be configured to send SLMs. In that case, the device can only generate SLRs for received SLM PDUs. The same is true for LMM/LMR also.

Use the no form of this command to disable sending SLR/LMR PDUs.

Command Syntax

```
ethernet cfm loss-measurement reply (slm | lmm)
no ethernet cfm loss-measurement reply (slm | lmm)
```

Parameters

slm	Synthetic Loss Messages
lmm	Loss Measurement Messages

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#ethernet cfm loss-measurement reply slm
```

ethernet cfm mep

Use this command to create a Maintenance End Point (MEP), make it active or inactive and enter Ethernet CFM MA MEP mode.

A MEP created with the `active false` option remains inactive and CFM functionality is suspended for such a MEP.

Note: For a VPWS instance, only an up MEP can be created; a down MEP cannot be created for VPWS.

Use the `no` form of this command to delete a MEP.

Command Syntax

```
ethernet cfm mep (up|down) mpid MEPID active (false|true) (local-vid VID|) ((uni-
  mep)|) (IFNAME | (vpws VCNAME) )
no ethernet cfm mep (up|down) mpid MEPID (local-vid VID|) (IFNAME | (vpws VCNAME) )
```

Parameters

`down`	Down MEP
`up`	Up MEP
`MEPID`	Host MEP identifier <1-8191>
`active`	Administrative state of the MEP
`true`	Make the MEP active
`false`	Make the MEP inactive
`VID`	Local VLAN identifier for the MEP, a secondary VLAN for the MA
`uni-mep`	UNI Maintenance Entity Group (MEG) MEP to intimate the UNI type
`IFNAME`	Interface name
`VCNAME`	Virtual circuit name

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#
```

ethernet cfm traceroute cache

use this command to set the cache size for traceroute output.

Use the no form of this command to set the cache size to its default (100).

Command Syntax

```
ethernet cfm traceroute cache size <1-4095> (bridge <1-32>|vpws)
no ethernet cfm traceroute cache size <1-4095> (bridge <1-32>|vpws)
```

Parameters

<1-4095>	Number of entries in cache
<1-32>	Bridge identifier
vpws	VPWS instance

Default

100 entries

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm traceroute cache size 1 bridge 1
(config)#ethernet cfm traceroute cache size 1 vpws
```

exit-ether-ma-mode

Use this command to exit Ethernet CFM MA mode and go back to Ethernet CFM mode.

Command Syntax

```
exit-ether-ma-mode
```

Parameters

None

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#exit-ether-ma-mode
```

exit-ether-ma-mep-mode

Use this command to exit Ethernet CFM MA MEP mode and go back to Ethernet CFM MA mode.

Command Syntax

```
exit-ether-ma-mep-mode
```

Parameters

None

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode
```

hardware-profile filter cfm-domain-name-str

Use this command to enable or disable setting the CFM domain name as a character string.

Command Syntax

```
hardware-profile filter cfm-domain-name-str (enable|disable)
```

Parameters

`enable`	Enable CFM domain name as a character string
`disable`	Disable CFM domain name as a character string

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#hardware-profile filter cfm-domain-name-str enable
```

intervals-stored

Use this command to set the number of frame loss measurement intervals to store in the history table.

Use the no form to set the number of measurement intervals to its default (32).

Command Syntax

```
intervals-stored <2-1000>
no intervals-stored
```

Parameters

<2-1000>	Time intervals

Default

32

Command Mode

Ethernet CFM loss measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm loss-measurement profile-name PROF1
(config-cfm-lm)#intervals-stored 50
```

loss-measurement type on-demand

Use this command to schedule an on-demand CFM loss measurement session.

Command Syntax

```
loss-measurement type on-demand profile-name WORD rmep (mac-address MAC|mep-id
  MEPID) start-time (immediate|relative HH:MM:SS|absolute HH:MM:SS <1-31> MONTH
  <1993-2035>) stop-time (none|relative HH:MM:SS|absolute HH:MM:SS <1-31> MONTH
  <1993-2035>) repetition-period <6000-4294967295> mep MEPID domain DOMAIN_NAME
  (vlan <2-4094> | bridge <1-32> | vpws VCNAME)
```

Parameters

`WORD`	Loss measurement profile name
`MAC`	Destination MAC address in HHHH.HHHH.HHHH format
`MEPID`	Remote MEP identifier <1-8191> to which to send the service OAM loss measurement frame
`start-time`	Measurement session start time
`immediate`	Start immediately
`relative HH:MM:SS`	Relative time to start from the current system time
`absolute HH:MM:SS <1-31> MONTH <1993-2035>`	Scheduled date and time to start; for the month, specify the first three letters
`stop-time`	Measurement session stop time
`none`	Never stop
`relative HH:MM:SS`	Relative time to stop from the current system time
`absolute HH:MM:SS <1-31> MONTH <1993-2035>`	Scheduled date and time to stop; for the month, specify the first three letters
`repetition-period`	Repetition time between measurement intervals
`<0-4294967295>`	Repetition time in seconds
`MEPID`	Remote MEP identifier <1-8191> to which to send the service OAM loss measurement frame
`DOMAIN_NAME`	Maintenance domain name
`<2-4094>`	Primary VLAN identifier of the MA
`<1-32>`	Bridge identifier
`VCNAME`	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#loss-measurement type on-demand profile-name slm rmep mac-address 0018.2323.1234
start-time immediate stop-time none repetition-period 9000 mep 201 domain 12345 vlan 10
bridge 1
#loss-measurement type on-demand profile-name slm rmep mac-address 0018.2323.1234
start-time immediate stop-time none repetition-period 9000 mep 201 domain 12345 vpws
ETH-2001
```

loss-measurement type proactive

Use this command to configure and start a proactive CFM loss measurement session.

Command Syntax

```
loss-measurement type proactive profile-name WORD rmep (mac-address MAC) mep MEPID
  domain DOMAIN_NAME (vlan <2-4094> | bridge <1-32> |vpws VCNAME)
```

Parameters

WORD	Loss measurement profile name
rmep	Remote MEP
MAC	Destination MAC address in HHHH.HHHH.HHHH format
MEPID	Remote MEP identifier <1-8191> to which to send the service OAM loss measurement frame
mep	MEP
MEPID	MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
<2-4094>	Primary VLAN identifier of the MA
<1-32>	Bridge identifier
VCNAME	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#loss-measurement type proactive profile-name slm rmep mac-address
0018.2323.1234 mep 201 domain 12345 vlan 10 bridge 1
#loss-measurement type proactive profile-name slm rmep mac-address
0018.2323.1234 mep 201 domain 12345 vpws ETH-2001
```

measurement-interval

Use this command to set the measurement interval for frame loss or delay measurement session.

Use the no form of this command to set the measurement interval to its default value (15 minutes).

Command Syntax

Loss measurement:

```
measurement-interval <1-525600>
no measurement-interval
```

Delay measurement:

```
measurement-interval <1-1440>
no measurement-interval
```

Parameters

For frame loss measurement:

<1-525600>	Measurement interval in minutes

For frame delay measurement:

<1-1440>	Measurement interval in minutes

Default

15 minutes

Command Mode

Ethernet CFM loss measurement mode and Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

Loss measurement:

```
#configure terminal
(config)#ethernet cfm loss-measurement profile-name PROF1
(config-cfm-lm)#measurement-interval 500
```

Delay measurement:

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)# measurement-interval 1
```

measurement-type slm

Use this command to generate Frame Loss Message (SLM/LMM) service OAM PDUs and track replies (SLR/LMR).

The measurement-type CCM is a dual-ended frame loss method in which generated CCM PDUs carry frame loss measurement information (TxFCf, RxFCb and TxFCb).

Use the no form of this command to set the measurement type to its default value (slm).

SLM and LMM cannot be enabled at the same time. All MEPs can use either LMM or SLM for frame loss measurement.

Command Syntax

```
measurement-type (slm | lmm | ccm)
no measurement-type
```

Parameters

`slm`	SLM service PDUs are generated and SLRs is tracked for frame loss measurement.
`lmm`	LMM service PDUs are generated and LMRs is tracked for frame loss measurement.
`ccm`	CCM PDUs are used for frame loss measurement which carries frame loss measurement information.

Command Mode

Ethernet CFM loss measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm loss-measurement profile-name PROF1
(config-cfm-lm)#measurement-type slm
```

mep crosscheck

Use this command to configure a remote MEP crosscheck.

Use the no form of this command to delete a crosscheck MEP.

Command Syntax

```
mep crosscheck mpid MEPID (mac MAC|)
no mep crosscheck mpid MEPID (mac MAC|)
```

Parameters

MEPID	Remote host MEP identifier <1-8191>
MAC	MAC address in HHHH.HHHH.HHHH format. This parameter is mandatory to send unicast Continuity Check Messages (CCMs). Otherwise, multicast CCMs are sent by default.

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#mep crosscheck mpid 51
```

mep lowest-priority-defect

Use this command to set the lowest-priority defect that can generate a fault alarm.

Use the no form of this command to set the lowest-priority defect to its default (`defMACstatus`).

Command Syntax

```
mep lowest-priority-defect
  (defRDICCM|defMACstatus|defRemoteCCM|defErrorCCM|defXconCCM)
no mep lowest-priority-defect
```

Parameters

`defRDICCM`	1 (lowest): At least one of the Remote MEP state machines is receiving valid CCMs from its remote MEP that has the Remote Defect Indication (RDI) bit set.
`defMACstatus`	2: One or more of the remote MEPs is reporting a failure in its Port Status Type-Length-Value (TLV) or Interface Status TLV: MEP Down.
`defRemoteCCM`	3: At least one of the remote MEP state machines is not receiving valid CCMs from its remote MEP.
`defErrorCCM`	4: One or more invalid CCMs has been received, and 3.5 times the CCMs' transmission interval has not yet expired.
`defXconCCM`	5: (highest): One or more cross-connect continuity check messages (CCMs) has been received, and 3.5 times at least one of those CCMs' transmission interval has not yet expired.

Default Value

defMACstatus

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe7
(config-ether-cfm-ma-mep)#mep lowest-priority-defect defRemoteCCM
```

message-period

Use this command to set the interval between loss or delay measurement OAM message transmission.

Use the no form of this command to set the interval between loss or delay measurement messages to its default value (1 second).

Command Syntax

Loss measurement:

```
message-period (1|2|3|4|5)
no message-period
```

Delay measurement:

```
message-period (1s|10s)
no message-period
```

Parameters

Loss measurement:

1	3 milliseconds
2	10 milliseconds
3	100 milliseconds
4	1 second
5	10 seconds

Delay measurement:

1s	1 second
10s	10 seconds

Default Value

1 second

Command Mode

Ethernet CFM loss measurement mode

Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

Loss measurement:

```
#configure terminal
(config)#ethernet cfm loss-measurement profile-name PROF1
(config-cfm-lm)#message-period 3
```

Delay measurement:

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)#message-period 10s
```

number-intervals-stored

Use this command to set the number of completed measurement intervals to store in the history statistic table for a two-way performance monitoring frame delay measurements on a specific MEP.

Use the no form to set the number of completed measurement intervals to store in the history statistic table for a two-way performance monitoring frame delay measurements on a specific MEP to its default (32).

Command Syntax

```
number-intervals-stored <2-1000>
no number-intervals-stored
```

Parameters

<2-1000>	Number of records to store in history

Default

32

Command Mode

Ethernet CFM delay measurement mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm delay-measurement profile-name PROF1
(config-cfm-dm)# number-intervals-stored 4
```

ping ethernet mac

Use this command to send a loopback message for a MAC address to a remote MEP for fault verification. Use either the `domain` or the `level` parameter with the `vlan` or `bridge` parameter to target a specific device.

Command Syntax

```
ping ethernet mac MACADDRESS unicast source MEPID (domain DOMAIN_NAME | level <0-
  7>) (vlan VLAN_ID | bridge <1-32> | vpws VCNAME)
```

Parameters

`MACADDRESS`	Destination MAC address in HHHH.HHHH.HHHH format
`MEPID`	Source host MEP ID <1-8191>
`DOMAIN_NAME`	Maintenance domain name of MEP
`<0-7>`	Level associated with the domain
`VLAN_ID`	Primary VLAN identifier <2-4094> of the MA
`<1-32>`	Bridge identifier
`VCNAME`	Virtual circuit name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#ping ethernet mac 0018.236e.5eb5 unicast source 201 domain 12345 vlan 10 bridge 1
success rate is  100 (5/5)

#ping ethernet mac 0018.236e.5eb5 unicast source 201 domain 12345 vpws ETH-2001
success rate is  100 (5/5)
```

rmep auto-discovery

Use this command to enable or disable whether MEPs are discovered automatically based on received CCMs (Continuity Checking Messages).

On disabling RMEP auto-discovery, a previously learned RMEP is removed.

Command Syntax

```
rmep auto-discovery enable|disable
```

Parameters

`enable`	Enable automatic RMEP discovery
`disable`	Disable automatic RMEP discovery

Default

disable

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#rmep auto-discovery enable
```

service ma-type

Use this command to create a service Maintenance Association (MA), with or without a VLAN, and enter Ethernet CFM MA mode

This command allows creation of a maintenance association for link-level MEPs (level 0) which do not listen on a VLAN.

A VID can be associated with an MA only at the time of MA creation. If an MA is created without a VID, a VID cannot be added to it during runtime because an MA without a VID is a link-level MA.

Use the no form of this command to remove an MA.

Command Syntax

```
service ma-type (string|integer|itu-t) ma-name MA_NAME (vlan VLAN_ID mip-creation
  (none|default|explicit|defer)
no service ma-name MA_NAME (vlan VLAN_ID mip-creation (none|default|explicit|defer)
```

Parameters

`ma-type`	Type of MA name (must match ethernet cfm domain-type `md-type` setting)
`string`	Character MA name. The `md-type` must be `character-string`.
`integer`	Integer MA name. The `md-type` must be `no-name`.
`itu-t`	ITU-T carrier code (ICC) format name defined by Y.1731.The `md-type` must be `integer`.
`MA_NAME`	MA name
`VLAN_ID`	Primary VLAN identifier <2-4094>
`mip-creation`	Maintenance domain Intermediate Point (MIP) creation permission for this domain
`none`	No MIP can be created for this VLAN identifier
`default`	MIP can be created if no lower active level or MEP at next lower active level
`explicit`	MEP is needed at the next lower active level
`defer`	Use the MIP creation permissions of the MD to which this MA belongs

Command Mode

Ethernet CFM mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe7
(config-ether-cfm-ma-mep)#
```

show ethernet cfm ais reception-status

Use this command to display information about the AIS (Alarm Indication Signal) frames received on a MEP.

Command Syntax

```
show ethernet cfm ais reception-status mep MEPID domain DOMAIN_NAME (vlan VLAN_ID|)
  (bridge <1-32>|)
```

Parameters

MEPID	Source host MEP ID <1-8191>
DOMAIN_NAME	Maintenance domain name of MEP
VLAN_ID	Primary VLAN identifier <2-4094> of the MA
<1-32>	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm ais reception-status mep 100 domain 12345 vlan 10 bridge 1
AIS frame is currently being received by MEP id 100

#show ethernet cfm ais reception-status mep 100 domain 12345 vlan 10 bridge 1
No AIS frame is being received by MEP 100
```

show ethernet cfm delay-measurement mep

Use this command to display delay measurement statistics for a MEP both for current and history or individually.

Command Syntax

```
show ethernet cfm delay-measurement mep MEPID domain DOMAIN_NAME (vlan <2-4094> |
  bridge <1-32> | vpws VCNAME) ((current-stats|history-stats)
```

Parameters

MEPID	Local MEP identifier<1-8191>
DOMAIN_NAME	Maintenance domain name of MEP
<2-4094>	VLAN identifier <2-4094>
<1-32>	Bridge identifier
VCNAME	Virtual circuit name
current-stats	Current session DB statistics.
history-stats	History DB statistics.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm delay-measurement mep  123 domain no_name vlan 10 bridge 1
 MEP                    : 123
 MA                     : 200
 VLAN ID                : 10
 Peer MAC Address       : 0000.0010.0000

CURRENT:
=====================
 Measurement ID : 2
 Measurement Type            : DMM
 Elapsed time(sec)           : 30
 Start Time                  : 2019 May 24 04:52:37
 Min Frame Delay(usec)       : 4
 Max Frame Delay(usec)       : 105
 Avg Frame Delay(usec)       : 81
 Min Inter FD Variation(usec): 34
 Max Inter FD Variation(usec): 34
 Avg Inter FD Variation(usec): 19

             FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
```

```
 1             0       - <    4999    3
 2             5000    - <    9999    0
 3             10000   - <     Inf    0

           INTER-FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    2
 2             5000    - <     Inf    0


HISTORY STATISTICS
======================
 MD                     : no_name
 MA                     : 200
 MEP                    : 123
 VLAN ID                : 10
 Measurement ID : 1
 Measurement Type            : DMM
 Elapsed time(sec)           : 60
 End Time                    : 2019 May 24 04:52:37
 Min Frame Delay(usec)       : 56
 Max Frame Delay(usec)       : 87
 Avg Frame Delay(usec)       : 67
 Min Inter FD Variation(usec): 1
 Max Inter FD Variation(usec): 31
 Avg Inter FD Variation(usec): 12

             FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    5
 2             5000    - <    9999    0
 3             10000   - <     Inf    0

           INTER-FRAME DELAY BINS
 Bin Number    Bin Threshold(usec)    Bin Counter
================================================
 1             0       - <    4999    4
 2             5000    - <     Inf    0
```

Table 3-53 explains the output fields.

Table 3-53: show ethernet cfm dm sessions

Field	Description
MEP	Local Maintenance End Point identifier
MA	Maintenance Association name

Table 3-53: show ethernet cfm dm sessions

Field	Description
Vlan Id	Primary vlan identifier of MA
DM-Profile	delay measurement profile name
Peer MAC Address	Peer's MAC address
Measurement ID	Id of the current or history session for that particular measurement interval
Measurement Type	One way or two way DM
Elapsed time	Time still left to complete the measurement interval
Start time	Time when DM session started
Min frame delay	Minimum delay recorded
Max frame delay	Max delay recorded
Avg frame delay	Average delay calculated
Min Inter FD Variation	Minimum inter frame delay variation calculated
Max Inter FD Variation	Maximum inter frame delay variation calculated
Avg Inter FD Variation	Average inter frame delay variation calculated
FRAME DELAY BINS	Frame delay bin configuration
INTER-FRAME DELAY BINS	Inter frame delay bin configuration
Bin Number	Bin number for which the threshold and counter is configured
Bin Threshold	A bin's configured threshold value
Bin counter	The number of delays recorded in this range
RMEP Id	Peer's MEP Id
End time	The time when the Measurement Interval was completed.
MD	Maintenance domain name

show ethernet cfm delay-measurement profile

Use this command to display information about a specified delay measurement profile or all configured delay measurement profiles.

Command Syntax

```
show ethernet cfm delay-measurement profile (WORD|)
```

Parameters

WORD	Profile name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#sh ethernet cfm delay-measurement profile dmm
Profile Name: dmm
 Measurement-type     -  DMM
 Measurement-interval -  1
 Message-period       -  10s
 Number of intervals stored -  4
 Bins per FD Interval       -  4
 Bins per IFDV Interval     -  3

       Frame Delay Bins
 Bin Number       Bin Threshold
  1               0
  2               1
  3               4

    Inter-Frame Delay Bins
 Bin Number       Bin Threshold
  1               0
  2               5000
```

Table 3-54 explains the output fields.

Table 3-54: show ethernet cfm delay-measurement profile

Field	Description
Profile Name	Loss measurement profile name
Measurement-type	DM session is one way or two way

Table 3-54: show ethernet cfm delay-measurement profile

Field	Description
Measurement-interval	See measurement-interval
message-period	See message-period
Number of intervals stored	See number-intervals-stored
Bins per FD Interval	See bins-per-fd-interval
Bins per IFDV Interval	See bins-per-ifdv-interval
Frame Delay Bins	Number of Frame Delay bins configured
Inter-Frame Delay Bins	Number of Inter-Frame Delay bins configured
Bin number	See bin-type
Bin threshold	See bin-type

show ethernet cfm dm sessions

Use this command to display information about the delay measurement session.

Command Syntax

```
show ethernet cfm dm sessions
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm dm sessions
MEP-Id  Status  StartTime           DM-Profile   Mac-address    Repetition Period(sec)
------------------------------------------------------------------------------------
123    Active  2019/06/01 13:14:46  123        0018.236e.5eb5     60
```

Table 3-55 explains the output fields.

Table 3-55: show ethernet cfm dm sessions

Field	Description
MEP-Id	Local Maintenance End Point identifier
Status	Inactive: if delay measurement session is not started Active: if delay measurement session is started
StartTime	Time when delay measurement session is started
DM-Profile	delay measurement profile name
Mac-address	MAC address
Repetition Period	Repetition time between measurement intervals in seconds

show ethernet cfm errors

Use this command to verify the defects present in a MEP.

Command Syntax

```
show ethernet cfm errors domain DOMAIN_NAME (bridge <1-32>|vpws)
```

Parameters

DOMAIN_NAME	Maintenance domain name
<1-32>	Bridge identifier
vpws	VPWS instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm errors domain 12345 bridge 1
Domain Name      Level     Vlan      MEPID      Defects
-------------------------------------------------------
12345             7        10        100        .....

#show ethernet cfm errors level 7 bridge 1
Domain Name      Level     Vlan      MEPID      Defects
-------------------------------------------------------
12345             7        10        100        .....

#show ethernet cfm errors level 7 vpws
Domain Name         Level         MEPID     Defects
-----------------------------------------------
12345               7         200       .....
```

Table 3-56 explains the output fields

Table 3-56: show ethernet cfm errors

Field	Description
Domain Name	Maintenance Domain name
Level	MD Level
Vlan	Vlan identifier
MEPID	Maintenance End Point identifier
Defects	Defects in current MEP

show ethernet cfm frame-lm session

Use this command to display information about the frame loss measurement session.

Command Syntax

```
show ethernet cfm frame-lm session
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm frame-lm session
MEPID  Status  StartTime           Lm-profile   Mac-address    Repetition Period(sec)
--------------------------------------------------------------------------------
201    Active  2018/10/01 00:18:46  slm        0018.236e.5eb5     60
```

Table 3-57 explains the output fields.

Table 3-57: show ethernet cfm frame-lm session

Field	Description
MEPID	Maintenance End Point identifier
Status	Inactive: if loss measurement is not in progress Active: otherwise
StartTime	When loss measurement started
Lm-profile	Loss measurement profile name
Mac-address	MAC address
Repetition Period	Repetition time between measurement intervals in seconds

show ethernet cfm loss-measurement mep

Use this command to display frame loss measurement statistics for a MEP.

Command Syntax

```
show ethernet cfm loss-measurement mep MEPID domain DOMAIN_NAME (vlan <2-4094> |
  bridge <1-32> | vpws VCNAME)
```

Parameters

MEPID	Host MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name of MEP
<2-4094>	VLAN identifier <2-4094>1
<1-32>	Bridge identifier.
VCNAME	Virtual circuit name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm loss-measurement mep 201 domain 12345 vlan 10 bridge 1
MEP: 201 MA: 43982
CURRENT:
 Measurement ID : 3
  Measurement Type           : slm
  Elapsed time(sec)          : 51
  Start Time                 : 2018 Nov 19 22:37:31
  Near End loss              : 0
  Far End loss               : 0
  Near End accumulated loss  : 0
  Far End accumulated loss   : 0

HISTORY:

 Measurement ID : 1
  Measurement Type           : slm
  Elapsed time(sec)          : 60
  End Time                   : 2018 Nov 19 22:36:31
  Near End loss              : 0
  Far End loss               : 0
  Near End accumulated loss  : 0
  Far End accumulated loss   : 0

 Measurement ID : 2
  Measurement Type           : slm
```

```
Elapsed time(sec)          : 60
End Time                   : 2018 Nov 19 22:37:31
Near End loss              : 0
Far End loss               : 0
Near End accumulated loss  : 0
Far End accumulated loss   : 0
```

Table 3-58 explains the output fields.

Table 3-58: show ethernet cfm loss-measurement mep

Field	Description
MEP	Maintenance End Point identifier
MA	Maintenance Association name
CURRENT:	Current loss measurement statistics
HISTORY:	Historic loss measurement statistics
Measurement ID	Sequence number
Measurement Type	See measurement-type slm
Elapsed time	Elapsed time in seconds
Start Time	Start time
End Time	End time
Near End loss	Near end loss
Far End loss	Far end loss
Near End accumulated loss	Near end accumulated loss
Far End accumulated loss	Far end accumulated loss

show ethernet cfm loss-measurement profile

Use this command to display information about a given loss measurement profile or all loss measurement profiles.

Command Syntax

```
show ethernet cfm loss-measurement profile WORD
```

Parameters

WORD	Profile name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm loss-measurement profile slm
Profile Name:slm
 measurement-type     -  slm
 measurement-interval -  1
 intervals-stored     -  3
 message-period       -  1
```

Table 3-59 explains the output fields.

Table 3-59: show ethernet cfm loss-measurement profile

Field	Description
Profile Name	Loss measurement profile name
measurement-type	See measurement-type slm
measurement-interval	See measurement-interval
intervals-stored	See intervals-stored
message-period	See message-period

show ethernet cfm ma status

Use this command to display the connectivity status of Maintenance Associations (MAs) in a domain.

Command Syntax

```
show ethernet cfm ma status domain DOMAIN_NAME (vlan <2-4094>|)
  (mep <1-8191>| mep all|) ((bridge <1-32>|vpws))
```

Parameters

DOMAIN_NAME	Maintenance domain name
<2-4094>	VLAN identifier
mep	Host MEP
<1-8191>	Host MEP identifier
all	All host MEPs
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm ma status domain 12345 vlan 10 bridge 1
MA NAME        VLAN                  STATUS
-----------------------------------------
  43982          10                  Active

#show ethernet cfm ma status domain 12345 vpws

MA NAME                   STATUS
------------------------------
  43981                   Active
```

Table 3-60 explains the output fields.

Table 3-60: show ethernet cfm ma status

Field	Description
MA NAME	Maintenance Association name

Table 3-60: show ethernet cfm ma status (Continued)

Field	Description
VLAN	VLAN identifier
STATUS	Active: All connected MEPs in MA are receiving the CCM with no defect or alarm present Partially Active: One or more connected MEPs in MA is not receiving CCM or it is receiving CCM with defect or alarm present Not Active: None of the connected MEPS in MA are receiving CCM or it is receiving CCM with defect or alarm present

show ethernet cfm maintenance-points local mep

Use this command to display information about the Maintenance End Points (MEPs) on a local interface.

Command Syntax

```
show ethernet cfm maintenance-points local mep (interface IFNAME|domain
  DOMAIN_NAME|level <0-7>) ((bridge <1-32>|vpws)|)
```

Parameters

IFNAME	Interface name
DOMAIN_NAME	Maintenance domain name
<0-7>	Maintenance level
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-point local mep level 7 bridge 1
MPID  Dir Lvl  VLAN  CC-Stat  HW-Status  CC-Intvl  MAC-Address    Def  Port  MD Name
------------------------------------------------------------------------------
100   Dn   7    10    Enable   Installed  100 ms   3c2c.99f0.b0c1  F    xe2   12345

#show ethernet cfm maintenance-points local mep domain 12345 bridge 1
MPID  Dir Lvl  VLAN  CC-Stat  HW-Status  CC-Intvl  MAC-Address    Def  Port  MD Name
------------------------------------------------------------------------------
100   Dn   7    10    Enable   Installed  100 ms   3c2c.99f0.b0c1  F    xe2   12345

#show ethernet cfm maintenance-points local mep level 7 vpws

MPID Dir Lvl CC-Stat HW-Status  CC-Intvl MAC-Address    Def Port  MD Name
------------------------------------------------------------------------
200  Up  7   Enable  Installed  3 ms     0018.23c8.f822 F   xe15  12345
```

Table 3-61 explains the output fields.

Table 3-61: show ethernet cfm maintenance-points local mep

Field	Description
MPID	MEP identifier
Dir	Up MEP or Down MEP

Table 3-61: show ethernet cfm maintenance-points local mep

Field	Description
Lvl	MD level
Vlan	VLAN identifier
CC-Stat	Whether continuity checking (CC) is enabled or disabled
HW-Status	Installed or pending to install in hardware
CC-Intvl	CCM Interval
MAC-Address	MAC address
Def	Defect present
Port	CFM interface
MD Name	MD name

show ethernet cfm maintenance-points local mip

Use this command to display information about the Maintenance Intermediate Points (MIPs) on a local interface.

Command Syntax

```
show ethernet cfm maintenance-points local mip (interface IFNAME|level <0-7>)
  (bridge <1-32>|)
```

Parameters

IFNAME	Interface name.
<0-7>	Maintenance level.
<1-32>	Bridge identifier.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-points local mip level 7 bridge 1
Level  VID   Type  Port   MAC-Address
------------------------------------------------------
7      10    MIP   xe3   0018.23ea.da36
7      10    MIP   xe5   0018.23ea.da38
```

Table 3-62 explains the output fields.

Table 3-62: show ethernet cfm maintenance-points local mip

Field	Description
Level	MD level
VID	VLAN identifier
Type	MIP
Port	Interface name
MAC-Address	MAC address

show ethernet cfm maintenance-points remote

Use this command to display information about a remote MEP.

Command Syntax

```
show ethernet cfm maintenance-points remote (mpid MEP_ID|) (domain
  DOMAIN_NAME|level LEVEL_ID) (vlan VLAN_ID|) ((bridge <1-32>|vpws)|)
```

Parameters

MEP_ID	Remote MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
LEVEL_ID	Maintenance level <0-7>
VLAN_ID	VLAN identifier <2-4094>
<1-32>	Bridge identifier
vpws	VPWS instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-points remote level 7 bridge 1
MEPID   RMEPID   LEVEL   VLAN    Rx CCM    RDI     PEER-MAC         TYPE
------------------------------------------------------------------------------
100     200        7      10       Yes    False   a82b.b579.fd2a   Configured

#show ethernet cfm maintenance-points remote domain 12345 bridge 1
MEPID   RMEPID   LEVEL   VLAN    Rx CCM    RDI     PEER-MAC         TYPE
------------------------------------------------------------------------------
100     200         7       10        Yes      False    a82b.b579.fd2a    Configured

#show ethernet cfm maintenance-points remote level 7 vpws
 MEPID     RMEPID     LEVEL     Rx CCM    RDI    PEER-MAC        TYPE
------------------------------------------------------------------------
 200       100        7         Yes       False  0018.236e.5ec2 Configured
```

Table 3-63 explains the output fields.

Table 3-63: show ethernet cfm maintenance-points remote

Field	Description
MEPID	MEP identifier
RMEPID	Remote MEP identifier
LEVEL	MD level

Table 3-63: show ethernet cfm maintenance-points remote

Field	Description
VLAN	VLAN identifier
Rx CCM	Yes if CCM receives, no if CCM doesn't receive.
RDI	Whether Remote Defect Indication (RDI) is on or off
PEER-MAC	Remote MEP mac address
TYPE	Configured or auto learned

show ethernet cfm statistics

Use this command to display CFM statistics: CCM sent and received, LBM sent and LBR received, LTM sent and LTR received.

Command Syntax

```
show ethernet cfm statistics mep MEPID domain DOMAIN_NAME vid VLANID
```

Parameters

MEPID	Host MEP identifier <1-8191>
DOMAIN_NAME	MD name
VLANID	Primary VLAN identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm statistics
Continuity Check Messages
   CCM Sent                : 168164
   CCM Received            : 165460

Loop Back Messages
   LBM Sent                : 5
   LBR Received(Valid)     : 5
   LBR Received(Bad msdu)  : 0
   LBR Received(Out-of-Seq): 0

Link Trace Messages
   LTM Sent                : 1
   LTR Sent                : 0
   LTR Received(Valid)     : 3
   LTR Received(unexpected): 0
```

Table 3-64 explains the output fields.

Table 3-64: show ethernet cfm statistics

Field	Description
Continuity Check Messages	
CCM Sent	Number of continuity check messsages (CCMs) sent
CCM Received	Number of CCMs received

Table 3-64: show ethernet cfm statistics

Field	Description
Loop Back Messages	
LBM Sent	Number of loopback messages (LBMs) sent
LBR Received(Valid)	Number of valid LBRs received
LBR Received(Bad msdu)	Number of LBRs received with bad MAC service data unit
LBR Received(Out-of-Seq)	Number of out-of-sequence LBRs received
Link Trace Messages	
LTM Sent	Number of link trace messages (LTMs) sent
LTR Received(Valid)	Number of link trace replies (LTRs) received
LTR Received(unexpected)	Number of unexpected LTRs received

show running-config cfm

Use this command to display CFM running configuration alone.

Command Syntax

```
show running-config cfm
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show running-config cfm
ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
 service ma-type string ma-name 43982 vlan 10 mip-creation none
   ethernet cfm mep down mpid 201 active true local-vid 10 xe2
     cc multicast state enable
     exit-ether-ma-mep-mode
   mep crosscheck mpid 18
   cc  interval 1
   exit-ether-ma-mode
!
```

traceroute ethernet

Use this command to start traceroute messages on a remote MEP.

Command Syntax

```
traceroute ethernet MAC mepid MEPID (domain DOMAIN | level <0-7>) (vlan VLANID |
  bridge <1-32> | vpws VCNAME)
```

Parameters

MAC	MAC address of the remote MEP or MIP in HHHH.HHHH.HHHH format.
MEPID	Host MEP identifier <1-8191>.
DOMAIN	MD name of the destination MEP or MIP.
<0-7>	Maintenance level to which remote MEP or MIP belongs.
VLANID	Primary VLAN identifier to which the destination MEP or MIP is associated.<2-4096>.
<1-32>	Bridge identifier.
VCNAME	Virtual circuit name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#traceroute ethernet 0018.236e.5eb8 mepid 201 domain 12345 vlan 10 bridge 1
MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress
action
0018.23ea.da36   1     RlyFDB                Ingress         IngOK
0018.23ea.da38   2     RlyFDB                Egress          EgrOK
0018.236e.5eb8   3     RlyHit                Ingress         IngOK

#traceroute ethernet 0018.236e.5eb8 mepid 201 domain 12345 vpws ETH-2001
MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress
action
0018.23ea.da36   1     RlyFDB                Ingress         IngOK
0018.23ea.da38   2     RlyFDB                Egress          EgrOK
0018.236e.5eb8   3     RlyHit                Ingress         IngOK
```

ethernet cfm test-signal profile-name

Use this command to create a test signal configuration profile associated with a specific MEP.

Use no form of this command to delete a test signal configuration profile.

Command Syntax

```
ethernet cfm test-signal profile-name WORD
no ethernet cfm test-signal profile-name WORD
```

Parameters

`profile-name`	Specify a profile-name
`WORD`	Specify the test signal profile name with max length of 64 characters

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm test-signal profile-name 123
(config-cfm-eth-tst)#

(config)#no ethernet cfm test-signal profile-name 123
```

test-signal mode

Use this command to enable an ETH test signal mode as generator or receiver or both.

Command Syntax

```
test-signal mode (generator|receiver|both)
```

Parameters

`generator`	The node will act as a ETH-TST frame generator
`receiver`	The node will act as a ETH-TST frame receiver
`both`	The node will act as both ETH-TST frame generator and receiver

Command Mode

Configure CFM ETH test mode

Default

The default test signal mode is receiver.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm test-signal profile-name 123
(config-cfm-eth-tst)#test-signal mode generator
```

test-signal test-type

Use this command to configure an ETH test signal test type is service interrupting or not.

Use no form of this command to delete the configured ETH test signal test type.

Command Syntax

```
test-signal test-type (in-service|out-of-service)
no test-signal test-type
```

Parameters

`in-service`	This indicates the ETH-Test is in-service and normal client service traffic is not interrupted
`out-of-service`	This indicates the ETH-Test is out-of-service and normal client service traffic is not disrupted

Command Mode

Configure CFM ETH test mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm test-signal profile-name 123
(config-cfm-eth-tst)#test-signal test-type in-service

(config-cfm-eth-tst)#no test-signal test-type
```

test-signal frame-size

Use this command to configure an ETH test signal frame size which is applicable only for generator test signal mode.

Use no form of this command to delete the configured ETH test signal frame size.

Command Syntax

```
test-signal frame-size <68-9600>
no test-signal frame-size
```

Parameters

<68-9600>	Specify the frame size within the range

Command Mode

Configure CFM ETH test mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm test-signal profile-name 123
(config-cfm-eth-tst)#test-signal frame-size 124

(config-cfm-eth-tst)#no test-signal frame-size
```

test-signal pattern-type

Use this command to configure the TLV type to be encoded in ETH-Test PDU.

Use no form of this command to reset the TLV pattern type to default.

Command Syntax

```
test-signal pattern-type (null-sig|null-sig-crc32|prbs|prbs-crc32)
no test-signal pattern-type
```

Parameters

`null-sig`	Specify test pattern as a Null signal without CRC-32
`null-sig-crc32`	Specify test pattern as a Null signal with CRC-32
`prbs`	Specify test pattern as a PRBS 2^31-1 without CRC-32
`prbs-crc32`	Specify test pattern as a PRBS 2^31-1 with CRC-32

Command Mode

Configure CFM ETH test mode

Default

Default TLV pattern type is Null signal.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm test-signal profile-name 123
(config-cfm-eth-tst)#test-signal pattern-type null-signal

(config-cfm-eth-tst)#no test-signal pattern-type
```

test-signal start-time

Use this command to start the ETH-Test session.

Command Syntax

```
test-signal start-time (relative START-TIME  | absolute START-TIME ) stop-time
  (relative STOP-TIME | absolute STOP-TIME) tst-profile-name WORD domain
  DOMAIN_NAME ma MA_NAME mep MEPID target (mac-address MAC|RMEPID) bridge <1-32>
```

Parameters

`start-time`	Specify Test session start time
`relative`	Specify Test session start time as relative
`absolute`	Specify Test session start time as absolute
`START-TIME`	Test session start time in minutes
`stop-time`	Specify Test session stop time
`STOP-TIME`	Test session stop time in minutes
`tst-profile-name`	
	Test session profile name
`WORD`	Specify test session profile name
`domain`	Specify domain
`DOMAIN_NAME`	The ID of maintenance domain of the MEP
`ma`	Specify ma
`MA_NAME`	The name of maintenance association name the MEP
`mep`	Specify mep
`MEPID`	Enter the MEPID ranging from <1-8191>
`target`	
`mac-address`	
`MAC`	
`RMEPID`	
`bridge <1-32>`	Specify the bridge ID

Command Mode

Exec mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#test-signal start-time relative 0 stop-time relative 30 tst-profile-name 123
domain 12345 ma 43982 mep 21 target mac-address 6cb9.c557.42d0 bridge 1
```

abort test-signal domain

Use this command to abort pre-configured test session.

Command Syntax

```
abort test-signal domain DOMAIN_NAME ma MA_NAME mep MEPID bridge <1-32>
```

Parameters

`domain`	Specify domain
`DOMAIN_NAME`	The ID of maintenance domain of the MEP
`ma`	Specify ma
`MA_NAME`	The name of maintenance association name the MEP
`mep`	Specify mep
`MEPID`	Enter the MEPID ranging from <1-8191>
`bridge <1-32>`	Specify the bridge ID

Command Mode

Exec mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#abort test-signal domain 12345 ma 43982 mep 21 bridge 1
```

show ethernet cfm test-signal profile

Use this command to display ETH-Test signal profile configuration.

Command Syntax

```
show ethernet cfm test-signal profile (WORD|)
```

Parameters

WORD	Specify the test signal profile name with max length of 64 characters

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ethernet cfm test-signal profile 123
  Profile Name      : 123
  Is Receiver       : False
  Is Generator      : True
  Test-Signal Type  : In-Service
  Frame Size(bytes) : 124
  Test Pattern Type : Null-Signal-Without-CRC-32
```

show ethernet cfm test-signal domain

Use this command to display ETH-Test receiver or generator statistics.

Command Syntax

```
show ethernet cfm test-signal domain DOMAIN_NAME ma MA_NAME mep MEPID bridge <1-32>
  stats (ctf|gtf)
```

Parameters

DOMAIN_NAME	The ID of maintenance domain of the MEP
ma	Specify ma
MA_NAME	The name of maintenance association name the MEP
mep	Specify mep
MEPID	Enter the MEPID ranging from <1-8191>
bridge 1	Bridge group name for bridging
stats	Display the statistics
ctf	Display ETH Test Frame Collector statistics
gtf	Display ETH Test Frame Generator statistics

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ethernet cfm test-signal domain 12345 ma 43982 mep 21 bridge 1 stats gtf
 TST Session status          : In-Progress
 Elapsed Time(sec)           : 36
 MD                          : 12345
 MA                          : 43982
 MEP                         : 21
 Peer MAC Address            : 6cb9.c557.42d0
 RMEP ID                     : 12
 Start Time                  : 2019 Mar 01 10:23:11
 Transmitted Packet Count    : 2854713
```

eth-lck state

Use this command to enable or disable ETH-Lock PDU transmission.

Command Syntax

```
eth-lck state (unlock|lock)
```

Parameters

`unlock`	Display ethernet lock PDU transmission
`lock`	Enable ethernet lock PDU transmission

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#eth-lck state lock
```

eth-lck message

Use this command to set the PDU MD level.

Command Syntax

```
eth-lck message level <0-7>
no eth-lck message level
```

Parameters

<0-7>	Set the level of the MD PDU.

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#eth-lck message level 2
```

eth-lck interval

Use this command to set/reset the PDU interval.

Command Syntax

```
eth-lck interval (1s|1m)
no eth-lck interval
```

Parameters

1s	Set the PDU interval in seconds.
1m	Set the PDU interval in minutes.

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#eth-lck interval 1s
```

eth-lck frame priority

Use this command to set/reset the PDU frame priority.

Command Syntax

```
eth-lck frame priority <0-7>
no eth-lck frame priority
```

Parameters

<0-7>	Set the PDU priority range.

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#eth-lck frame priority 3
```

show ethernet cfm lck statistics

Use this command to display a CFM lock statistics for a MEP.

Command Syntax

```
show ethernet cfm lck statistics mep MEPID domain DOMAIN_NAME (bridge <1-32>)
```

Parameters

`domain`	Specify domain
`DOMAIN_NAME`	The ID of maintenance domain of the MEP
`mep`	Specify mep
`MEPID`	Enter the MEPID ranging from <1-8191>
`bridge <1-32>`	Specify the bridge ID

Command Mode

Exec mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ethernet cfm lck statistics mep 151 domain 12345 bridge 1
MPID MD Name MA Name Lck State Rx Status Tx Rx
-----------------------------------------------
151  12345   200     True      False     7  0
```

show ethernet cfm lck details domain

Use this command to display a CFM lock user configuration.

Command Syntax

```
show ethernet cfm lck details domain DOMAIN_NAME ma MA_NAME mep MEPID (bridge <1-
  32>)
```

Parameters

`domain`	Specify domain
`DOMAIN_NAME`	The ID of maintenance domain of the MEP
`ma`	Specify ma
`MA_NAME`	The name of maintenance association name the MEP
`mep`	Specify mep
`MEPID`	Enter the MEPID ranging from <1-8191>
`bridge <1-32>`	Specify the bridge ID

Command Mode

Exec mode

Default

None

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ethernet cfm lck details domain 12345 ma 200 mep 151 bridge 1

Maintenance Domain              : 12345
Maintenance Association         : 200
MEP ID                          : 151
LCK PDU state                   : Locked
LCK Message Level               : 7
LCK PDU Interval                : 1 min
LCK PDU Priority                : 3
```

CHAPTER 4 G.8032 ERPS Version 2 Commands

This chapter contains the G.8032 (2012) Ethernet Ring Protection Switching (ERPS) version 2 commands.

bridge g8032 physical-ring

Use this command to create a physical ring and associate east and west interfaces with it. All ERP instances on this ring have the same east and west interfaces,

Use the no form of this command to delete a physical ring.

Command Syntax

```
bridge (<1-32> | backbone) g8032 physical-ring RINGNAME east-interface IFNAME
  west-interface IFNAME
no bridge (<1-32> | backbone) g8032 physical-ring RINGNAME
```

Parameters

bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.
physical-ring	Physical ring.
RINGNAME	Physical ring name (maximum 37 characters).
east-interface	East interface.
IFNAME	East interface name.
west-interface	West interface.
IFNAME	West interface name.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#bridge 1 g8032 physical-ring ring1 east-interface eth1 west-interface
eth2
(config)#no bridge 1 g8032 physical-ring ring1 disable
```

enable revertive

Use this command to set the revertive behavior of the ring node.

Command Syntax

```
enable (revertive | non-revertive)
```

Parameters

`revertive`	Revertive behavior.
`non-revertive`	Non-revertive behavior.

Command Mode

G.8032 profile configure mode

Examples

```
(g8032-profile-config)#enable revertive
```

force-switch|manual-switch

Use this command to configure administrative commands.

Command Syntax

```
(((force-switch|manual-switch)(east-interface|west-interface))|clear)
```

Parameters

`force-switch`	Forcefully block a ring port.
`manual-switch`	Manually block a ring port.
`east-interface`	Apply command to east interface.
`west-interface`	Apply command to west interface.
`clear`	Cancel a command.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#force-switch east-interface
```

g8032 erp-instance

Use this command to create an ERP instance and change to G.8032 configure switch mode.

Use the no form of this command to delete an ERP instance.

Command Syntax

```
g8032 erp-instance INSTANCENAME bridge (<1-32> | backbone)
no g8032 erp-instance INSTANCENAME bridge (<1-32> | backbone)
```

Parameters

INSTANCENAME	Instance name (maximum 32 characters).
bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#g8032 erp-instance instance1 bridge 1
(g8032-config-switch)#
```

g8032 profile

Use this command to create a profile on a bridge and switch to G.8032 profile configure mode.

Use the no form of this command delete a profile on a bridge.

Command Syntax

```
g8032 profile PROFILENAME bridge (<1-32> | backbone)
no g8032 profile PROFILENAME bridge (<1-32> | backbone)
```

Parameters

PROFILENAME	Profile name (maximum 32 characters).
bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#g8032 profile profile123 bridge 1
(g8032-profile-config)#
```

level

Use this command to set the maintenance entity group (MEG) level (MEL) to carry in R-APS messages.

Command Syntax

```
level <0-7>
```

Parameters

<0-7>	Level.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#level 2
```

non-virtual-channel

Use this command to make a sub-ring function without a virtual channel.

Use the no form of this command to delete a non-virtual channel.

Command Syntax

```
non-virtual-channel
no non-virtual-channel
```

Parameters

None

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#non-virtual-channel
```

physical-ring

Use this command to associate the ERP instance to a physical ring.

Command Syntax

```
physical-ring RINGNAME
```

Parameters

RINGNAME	Physical ring name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#physical-ring ring1
```

profile name

Use this command to associate the ERP instance to a profile.

Command Syntax

```
profile name PROFILENAME
```

Parameters

PROFILENAME	Profile name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#profile prof_1
```

ring-id

Use this command to set the ring identifier.

Command Syntax

```
ring-id <1-255>
```

Parameters

<1-255>	Ring identifier.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#ring-id 1
```

rpl role

Use this command to set the RPL (Ring Protection Link) role of the ring node.

Command Syntax

```
rpl role ((owner | neighbor | next-neighbor)(east-interface | west-interface) |
  non-owner )
```

Parameters

`owner`	Ring node is the RPL owner.
`neighbor`	Ring node is neighbor to the RPL owner.
`next-neighbor`	Ring node is neighbor to the neighbor of the RPL owner.
`east-interface`	Role assigned to east interface.
`west-interface`	Role assigned to west interface.
`non-owner`	Ring node does not own the RPL.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#rpl role owner east-interface
```

show g8032 erp-instance

Use this command to display details about an ERP instance.

Command Syntax

```
show g8032 erp-instance INSTANCENAME bridge (<1-32>|backbone)
```

Parameters

INSTANCENAME	Instance name.
bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.

Command Mode

Configure mode

Example

```
(config)#show g8032 erp-instance instance1 bridge 1
Inst Name  : instance1
State      : G8032_ST_INIT
Phy Ring   : -
Role       : -
East Link  : -
West Link  : -
Attached   : -
Attached To: -
Virt Chan  : -
-------------------------------------------------------------

     Channel        |    Interface           |  Profile
 (LEVL, VID, RID)   | (east,ver), (west,ver) |
=========================================================
 (7, 4065, 135)     | (eth11,1),  (eth2,2)   | PROF1
=========================================================
Data Traffic: 1,2,3,10,12...
```

show g8032 physical-ring

Use this command to display details about a physical ring.

Command Syntax

```
show g8032 physical-ring RINGNAME bridge (<1-32>|backbone)
```

Parameters

RINGNAME	Ring name.
bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.

Command Mode

Configure mode

Examples

```
(config)#show g8032 physical-ring ring1 bridge1
Ring     : ring1
==========
Bridge   : 1
East     : eth1
West     : eth2
ERP Inst : inst1, inst2, inst3
```

show g8032 profile

Use this command to display details about a profile.

Command Syntax

```
show g8032 profile PROFILENAME bridge (<1-32>|backbone)
```

Parameters

PROFILENAME	Profile name.
bridge	Bridge.
<1-32>	Bridge identifier.
backbone	Backbone bridge.

Command Mode

Configure mode

Examples

```
(config)#show g8032 profile profile1 bridge 1
Profile : profile1
=========
 Wait-To-Restore : 5 mins
 Hold Off Timer  : 0 secs
 Guard Timer     : 500 ms
 Wait-To-Block   : 5500 ms
 Protection Type : Revertive
```

sub-ring

Use this command to make the ERP instance a sub-ring. You should only give this command on interconnection nodes.

Use the no form of this command to make the ERP instance a major ring.

Command Syntax

```
sub-ring block (east-interface|west-interface)
no sub-ring
```

Parameters

`east-interface`
: Block east interface.

`west-interface`
: Block west interface.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#sub-ring block east-interface
```

tcn-propogation

Use this command to enable or disable TCN (topology change notification) propagation for an interconnected ring.

Command Syntax

```
tcn-propogation (enable|disable)
```

Parameters

`enable`	Enable TCN propagation.
`disable`	Disable TCN propagation.

Command Mode

Configure mode

Examples

```
(config)#tcn-propogation enable
```

timer

Use this command to set timers.

Command Syntax

```
timer (wait-to-restore (<1-12>|default) | hold-off (<0-100>|default) | guard-timer
  (<1-200>|default))
```

Parameters

`wait-to-restore`	Wait-to-restore timer used to verify that a signal failure is not intermittent.
`<1-12>`	Timer value in minutes.
`default`	Default value of timer <5>.
`hold-off`	Hold-off timer used to filter intermittent link faults.
`<0-100>`	Timer value in a multiple of 100 milliseconds.
`default`	Default value of timer <0>.
`guard-timer`	Guard timer that blocks latent outdated messages from causing unnecessary state changes.
`<1-200>`	Timer value in a multiple of 10 milliseconds.
`default`	Default value of timer <50>.

Command Mode

G.8032 profile configure mode

Examples

```
(g8032-profile-config)#timer wait-to-restore 7
(g8032-profile-config)#timer hold-off 50
(g8032-profile-config)#timer guard-timer 30
```

version

Use this command to set the version to carry in R-APS messages for an interface.

Command Syntax

```
version <0-1> (east-interface | west-interface)
```

Parameters

`<0-1>`	Version:
`0`	ITU-T Recommendation G.8032/Y.1344 2008
`1`	ITU-T Recommendation G.8032/Y.1344 2012
`east-interface`	Assigned to east interface.
`west-interface`	Assigned to west interface.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#version 1 east-interface
```

virtual-channel

Use this command on a sub-ring to attach it to a major instance.

Use the no form of this command to delete a virtual channel.

Command Syntax

```
virtual-channel (<2-4094>|) attached-to-instance INSTANCENAME
no virtual-channel
```

Parameters

`<2-4094>`	VLAN identifier.
`INSTANCENAME`	Major instance name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#virtual-channel 3 attached-to-instance inst1
```

vlan

Use this command to add a VLAN to the ERP instance and set its type.

Use the no forms of this command to disassociate a VLAN from the ERP instance.

Command Syntax

```
vlan <2-4094> (raps-channel | data-traffic)
no raps-channel
no data-traffic <2-4094>
```

Parameters

`<2-4094>`	VLAN identifier.
`raps-channel`	Direct R-APS traffic on this VLAN.
`data-traffic`	Direct data traffic on this VLAN.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#vlan 3 raps-channel
```

SECTION 9

Trigger Fail-Over

Trigger Failover Configuration Guide

Contents

This document contains this chapter:

CHAPTER 1 Trigger Failover Configuration

This chapter contains Trigger Failover (TFO) configuration examples.

This example shows the complete configuration to enable TFO in a simple network topology. TFO complements NIC teaming functionality supported on blade servers. TFO allows a switch module to monitor specific uplink ports to detect link failures. When the switch module detects a link failure, it disables the corresponding downlink ports automatically.

TFO uses these components:

- A Fail Over Group (FOG) contains a Monitor Port Group (MPG) and a Control Port Group (CPG).
- An MPG contains only uplink ports.
- A CPG contains only downlink ports.

Note:

- TFO is supported in STP or RSTP bridge mode.
- TFO can be configured on a LAG interface.

Basic Configuration

Figure 1-94: Basic topology

Switch

`#configure terminal`	Enter configure mode.
`(config)#tfo enable`	Enable TFO globally.
`(config)#fog 1 enable`	Create a Fail over group (FOG) and enable it.
`(config)#interface xe35`	Enter interface mode
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#fog 1 type mpg`	Specify the MPG member for FOG 1.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe34`	Enter interface mode
`(config-if)#link-type downlink`	Specify the link-type as Downlink.
`(config-if)#fog 1 type cpg`	Specify the CPG member for FOG 1.
`(config-if)#end`	Exit interface and configure mode

Validation

```
#show tfo

TFO : Enable

Failover Group 1 : Enable
```

```
No. of links to trigger failover : 0
MPG Port : xe35
CPG Port : xe34
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
#
```

Port-Channel Configuration

Topology

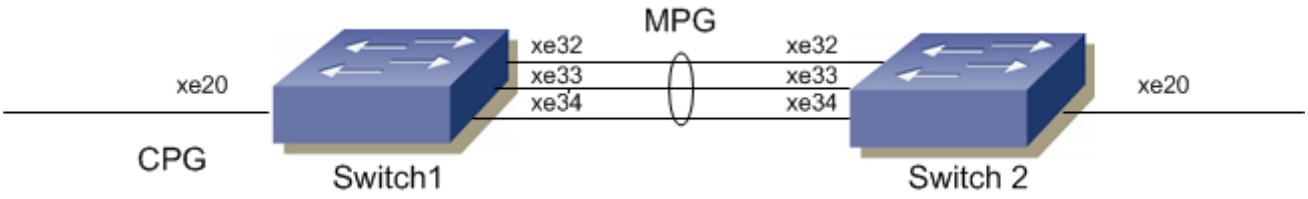


Figure 1-95: TFO with port-channel

Switch 1

`#configure terminal`	Enter configure mode.
`(config)#tfo enable`	Enable TFO globally.
`(config)#fog 1 enable`	Create a Fail over group (FOG) and enable it.
`(config)#interface po1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer2.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe32`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer2.
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#channel-group 1 mode active`	Specify the channel group in interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe33`	Enter interface mode
`(config-if)#switchport`	Make the interface as Layer2.
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#channel-group 1 mode active`	Specify the channel group in interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe34`	Enter interface mode
`(config-if)#switchport`	Make the interface as Layer2.
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#channel-group 1 mode active`	Specify the channel group in interface
`(config-if)#exit`	Exit interface mode

(config)#interface xe20	Enter interface mode
(config-if)#link-type downlink	Specify the link-type as Downlink.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter port-channel mode
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#end	Exit interface and configure mode

Switch 2

#configure terminal	Enter configure mode.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#exit	Exit interface mode
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode

Validation

```
#show interface brief | include up
xe20        ETH   --    --                up      none    10g   --
xe32        ETH   --    --                up      none    10g   --
xe33        ETH   --    --                up      none    10g   --
xe34        ETH   --    --                up      none    10g   --
eth0          METH            up      --      100m
lo                                              up          --
lo.management                                   up          --


#show tfo

TFO : Enable

Failover Group 1 : Enable
No. of links to trigger failover : 0
```

```
    MPG Port : po1
    CPG Port : xe20
    No. of times MPG link failure : 0
    No. of times MPG link recovered : 0
    No. of times CPG got auto disabled : 0
    No. of times CPG got auto enable : 0
```

Trigger Failover Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Trigger Failover Commands

This chapter describes the trigger failover (TFO) commands.

clear tfo counter

Use this command to clear the TFO counters. If you do not specify a parameter, this command clears counters for all FOG indexes.

Command Syntax

```
clear tfo counter
clear tfo counter fog <1-64>
```

Parameters

<1-64>	Clear counters for this Failover Group Index

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tfo counter
```

fog

Use this command to:

- Create or delete a failover group (FOG)
- Enable or disable an exisitng FOG

Even if FOG index do not exit, FOG can be created as enabled with “enable” option in CLI.

If the FOG index already exists:

- When the FOG status is disabled and Control Port Group (CPG) links are previously disabled (because of TFO), then the links are enabled. If a particular CPG member belongs to multiple CPGs, then this CPG member is enabled only if all corresponding Monitor Port Groups (MPG) are enabled.
- When the FOG status is enabled and MPG is down, then the corresponding CPG links are disabled.

Use the `no` form of this command to delete a FOG.

Command Syntax

```
fog <1-64> (enable|disable)
no fog <1-64>
```

Parameters

`<1-64>`	Failover Group Index
`enable`	Enable Failover Group
`disable`	Disable Failover Group

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#fog 5 enable
```

fog tfc

Use this command to set the number of links to trigger failover for a Monitor Port Groups (MPG).

Command Syntax

```
fog <1-64> tfc <0-63>
```

Parameters

<1-64>	Failover Group index
<0-63>	Trigger failover count

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#fog 5 tfc 7
```

fog type

Use this command to map upstream/downstream links in a FOG as a Monitor Port Group (MPG) or Control Port Group (CPG).

Use the no form of this command to unmap upstream/downstream links.

Command Syntax

```
fog <1-64> type (mpg|cpg)
no fog <1-64> type (mpg|cpg)
```

Parameters

<1-64>	Failover Group Index
mpg	Map the interface to an MPG
cpg	Map the interface to a CPG

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#fog 5 type mpg
```

link-type

Use this command to make a port an uplink or downlink.

Use the no form of this command to remove the configuration.

Command Syntax

```
link-type (uplink|downlink)
no link-type
```

Parameters

`uplink`	Make the port an uplink
`downlink`	Make the port a downlink

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#link-type downlink
```

show tfo

Use this command to display FOG configuration and statistics.

Command Syntax

```
show tfo
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tfo

TFO : Enable

Failover Group 1 : Enable
No. of links to trigger failover : 0
MPG Port : xe1
CPG Port : xe18
No. of times MPG link failure : 0
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 0
No. of times CPG got auto enable : 0
```

Table 1-65 Explains the show command output fields.

Table 1-65: show tfo output fields

Field	Description
Failover Group	Enable the failover group.
No. of links to trigger failover	Number of links to trigger the failover group.
MPG Port	Details of the monitor port group.
CPG Port	Details of the control port group.

tfo

Use this command to enable or disable trigger failover (TFO). TFO can be enabled only if the bridge mode is STP or RSTP.

Command Syntax

```
tfo (enable|disable)
```

Parameters

`enable`	Enables Trigger failover
`disable`	Disables Trigger failover

Default

By default, TFO is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#tfo enable
```

SECTION 10 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 VRRP Configuration

This chapter provides an overview of Virtual Router Redundancy Protocol (VRRP) and its implementation with OcNOS. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

OcNOS only supports VRRP protocol version 3.

Terminology

Terms related to VRRP configuration are defined in the table below.

Backup Router	The VRRP router that is backing up an IP address. It assumes forwarding responsibility for the virtual IP address if the Master fails.
Critical IP	The IP address that a VRRP router sends/receives messages on for a particular session.
IP Address Owner	The VRRP Router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
Master Router	The VRRP router that owns the IP address (i.e., is being backed up), and which is the default router for forwarding for that IP address.
Virtual IP	The IP address that is being backed up by a VRRP session.
Virtual Router	A router managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP addresses across a common LAN. A VRRP Router might backup one or more virtual routers.
VRRPv2 Router	A router running the Virtual Router Redundancy Protocol version 2. It might participate in one or more virtual routers.
VRRPv3 Router	A router running the Virtual Router Redundancy Protocol version 3. It might participate in one or more virtual routers.

VRRP Process

Typically, end hosts are connected to the enterprise network through a single router (first-hop router) that is in the same Local Area Network (LAN) segment. The most popular method of configuration is for the end hosts to configure statically this router as their default gateway. This minimizes configuration and processing overhead. As shown in Figure 1-96, the problem with this configuration is that it produces a single point of failure if this first-hop router fails.

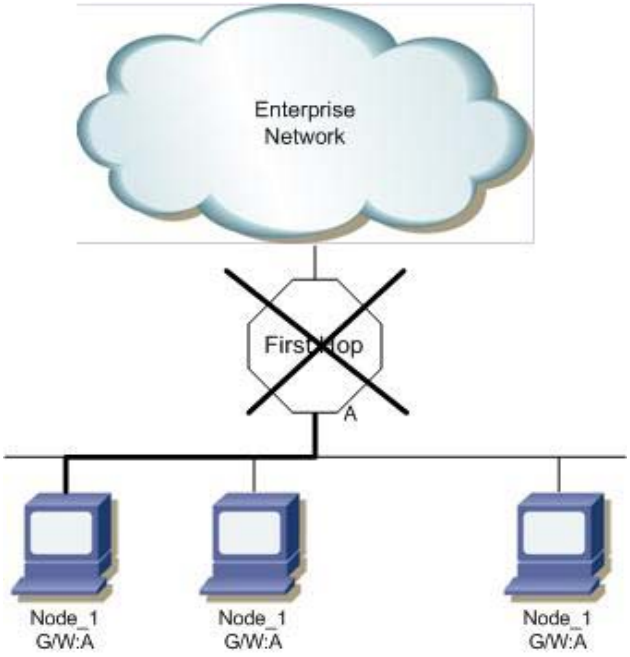


Figure 1-96: VRRP Process - First-Hop Not Reachable

The Virtual Router Redundancy Protocol attempts to solve this problem by introducing the concept of a virtual router, composed of two or more VRRP routers on the same subnet as shown in Figure 1-97. The concept of a virtual IP address is also introduced, which is the address that end hosts configure as their default gateway. One of the routers called the “Master” forwards packets on behalf of this IP address.

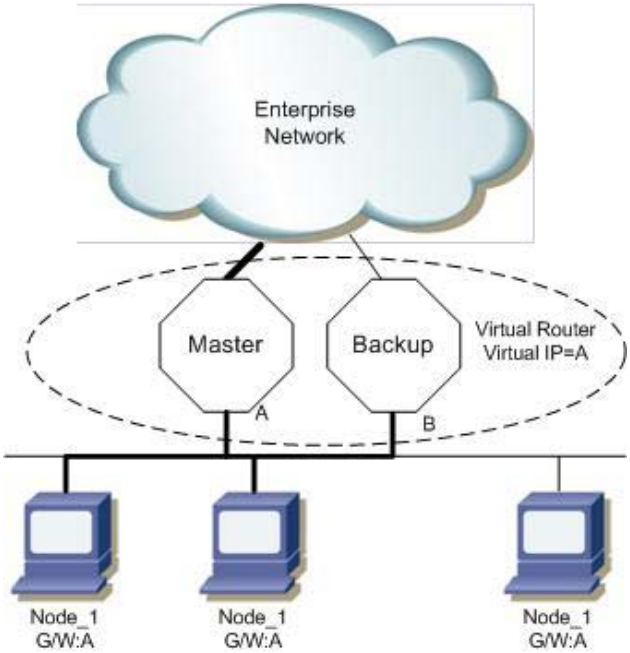


Figure 1-97: VRRP Process - Master and Backup VR

As shown in Figure 1-98, if the Master router fails, one of the other routers (Backup) assumes forwarding responsibility for it.

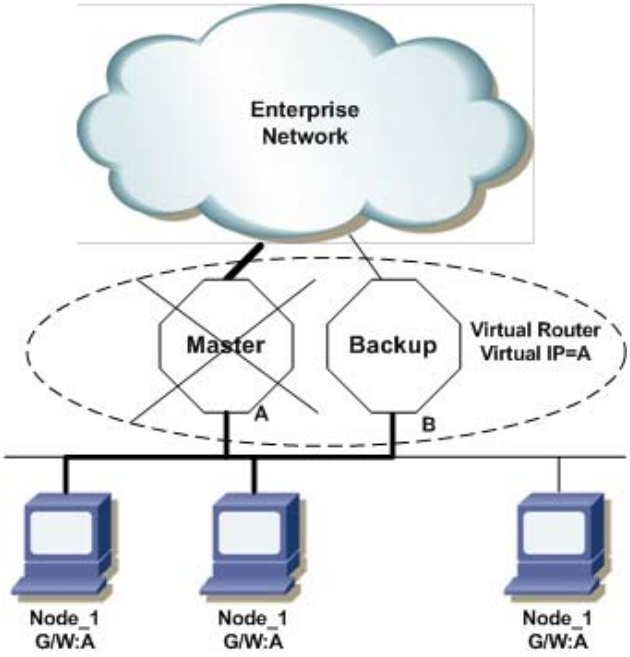


Figure 1-98: VRRP Process - Master Down and Backup Takeover

At first glance, the configuration in might not seem very useful, as it doubles the cost, and leaves one router idle at all times. This, however, can be avoided by creating two virtual routers and splitting the traffic between them.

Note: Adding a default route in the kernel on the interface that is used for VRRP might cause loss of network connectivity. According to the VRRP guidelines, when the VRRP session changes, the MAC address for the machine that attains the master state also changes. The change causes the default route from the kernel to disappear and leads to loss of connectivity. To avoid this situation, add the default route in the NSM and not in the kernel. This ensures that the default route remains on the machine across changes in the VRRP state.

To add default route through NSM, run the following command in NSM:

```
ip route 0.0.0.0/0 <IPADDRESS>
```

where `<IPADDRESS>` is the IP address of the default gateway.

One Virtual Router

In this configuration, the end-hosts install a default route to the IP address of virtual router 1(VRID = 1), and both routers R1 and R2 run VRRP. R1 is configured to be the Owner for virtual router 1 (VRID = 1) and R2 as a Backup for virtual router 1. If R1 fails, R2 will take over virtual router 1 and its IP addresses, and provide uninterrupted service for the hosts. Configuring only one virtual router doubles the cost, and leaves R2 idle at all times.

Topology

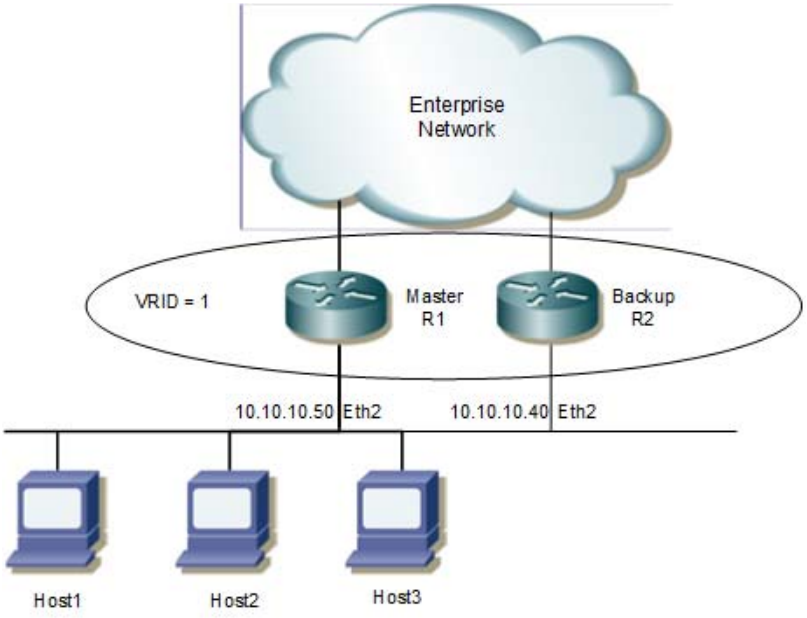


Figure 1-99: VRRP with One Virtual Router

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.50 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.50`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session on the router.

Validation

R1

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.50 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.50
 Operational master IP address: 10.10.10.50
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 45 seconds (4500 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R1#
```

R2

```
R2#show vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.50 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.40
 Operational master IP address: 10.10.10.50
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 21 seconds (2100 centi sec)
 Skew time: 21 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
```

```
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R2#
```

Two Virtual Routers

In the previous, one virtual router example, R2 is not backed up by R1. This example illustrates how to back up R2 by configuring a second virtual router. In this configuration, R1 and R2 are two virtual routers, and the hosts split their traffic between R1 and R2. R1and R2 functions as backups for each other.

Topology

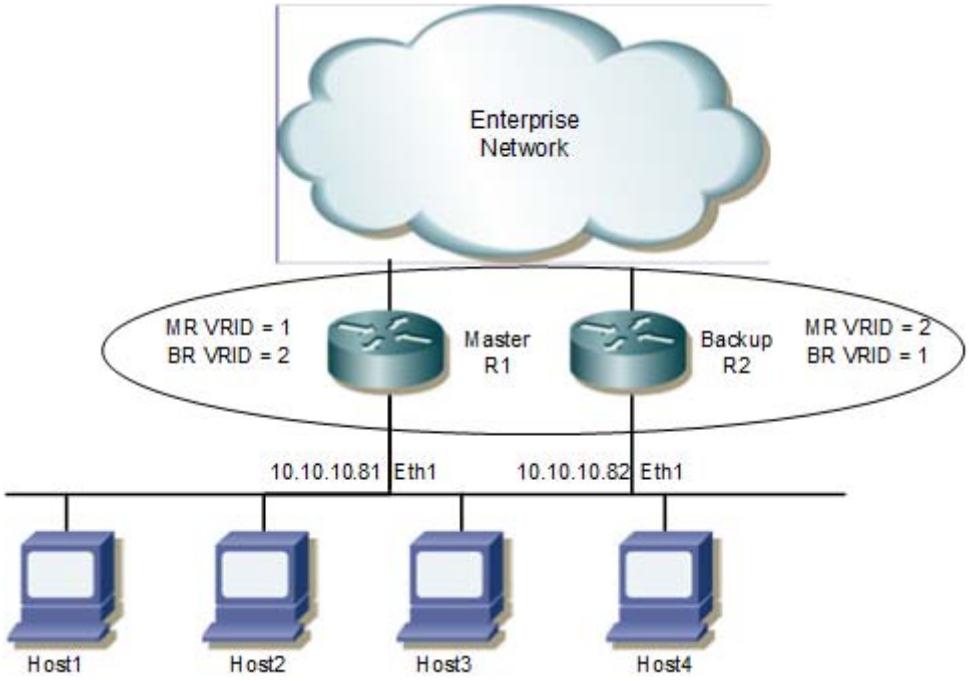


Figure 1-100: Configuring VRRP with Two Virtual Routers

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth1`	Create a VRRP instance for interface eth1.
`(config-router)#virtual-ip 10.10.10.81 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session 1 on the router.
`(config-router)#exit`	Exit `Router` mode and enter the `Configure` mode.

(config)#router vrrp 2 eth1	Create a VRRP instance for interface eth1.
(config-router)#virtual-ip 10.10.10.82	Set the virtual IP address for the VRRP session.
(config-router)#priority 200	Configure the priority to 200 (less than 255), because R2 is the Backup router.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#enable	Enable the VRRP session two on the router.

R2

#configure terminal	Enter the Configure mode.
(config)#router vrrp 1 eth1	Create a VRRP instance for interface eth1.
(config-router)#virtual-ip 10.10.10.81	Set the virtual IP address for the VRRP session.
(config-router)#priority 200	Configure the priority to 200 (less than 255), because R2 is the Backup router.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#enable	Enable the VRRP session 1 on the router.
(config-router)#exit	Exit the Router mode and enter the Configure mode.
(config)#router vrrp 2 eth1	Create a VRRP instance for interface eth1
(config-router)#virtual-ip 10.10.10.82 owner	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#enable	Enable the VRRP session two on the router.

Validation

The following outputs on R1and R2 display the complete configuration for each session on R1 and R2. In session one, R1 is the master router, and in session two R2 is the master router.

R1

```
R1#sh vrrp 1 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Master
```

```
 Virtual IP address: 10.10.10.81 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.81
 Operational master IP address: 10.10.10.81
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 1 minutes 25 seconds (8500 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R1#sh vrrp 2 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 2 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.82 (Not-owner)
 Virtual MAC address is 0000.5e00.0102
 Operational primary IP address: 10.10.10.81
 Operational master IP address: 10.10.10.82
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Skew time: 21 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R1#
```

R2

```
R2#sh vrrp 1 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.81 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.82
```



```
 Operational master IP address: 10.10.10.81
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 37 seconds (3700 centi sec)
 Skew time: 21 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R2#sh vrrp 2 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 2 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.82 (Owner)
 Virtual MAC address is 0000.5e00.0102
 Operational primary IP address: 10.10.10.82
 Operational master IP address: 10.10.10.82
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 12 seconds (1200 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: FALSE

R2#
```

Two Backup Routers

In this configuration, Host B could be a gateway router. As such, interface eth1 on Routers R1, R2, and R3, and the gateway router, would run the IGP protocol.

Topology

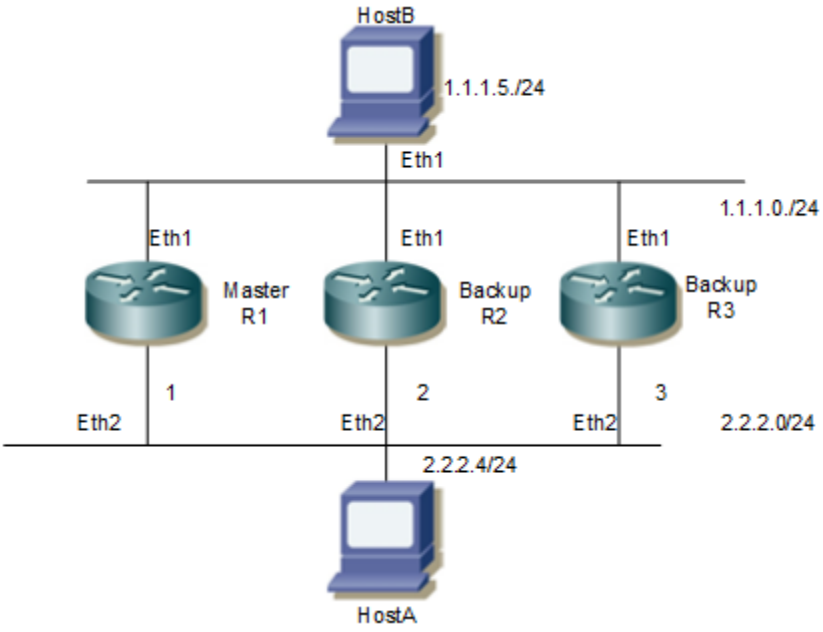


Figure 1-101: Configuring VRRP with Two Backup Routers

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address for interface eth2 to be in network 0.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#ip address 1.1.1.1/24`	Configure the IP address for interface eth1 to be in network 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 2.2.2.1 owner`	Configure R1 as the owner.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.

(config-if)#ip address 2.2.2.2/24	Configure the IP address for interface eth2 to be in network 0.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ip address 1.1.1.2/24	Configure the IP address for interface eth1 to be in network 1.
(config-if)#exit	Exit interface mode.
(config)#router vrrp 1 eth2	Create a VRRP instance for interface eth2.
(config-router)#virtual-ip 2.2.2.1	Configure R2 as the backup.
(config-router)#advertisement-interval 100	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
(config-router)#priority 100	Set the default value for the backup router.
(config-router)#preempt-mode true	Set true as the default value for the field.
(config-router)#enable	Enable the VRRP session on the router.
(config-router)#exit	Exit Router mode.

R3

#configure terminal	Enter the Configure mode.
(config)#interface eth2	Enter interface mode for eth2.
(config-if)#ip address 2.2.2.3/24	Configure the IP address for interface eth2 to be in network 0.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ip address 1.1.1.3/24	Configure the IP address for interface eth1 to be in network 1.
(config-if)#exit	Exit interface mode.
(config)#router vrrp 1 eth2	Create a VRRP instance for interface eth2.
(config-router)#virtual-ip 2.2.2.1	Configure R3 as the backup.
(config-router)#advertisement-interval 100	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
(config-router)#priority 254	Configure the priority for R3. The configurable range is 1-255.
(config-router)#preempt-mode true	Set true as the default value for the field.
(config-router)#enable	Enable the VRRP session on the router.
(config-router)#exit	Exit Router mode.

Validation

Router 1

```
R1#show vrrp
VRRP Version: 3
VMAC enabled
```

```
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 2.2.2.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 9 minutes 6 seconds (54600 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: FALSE
```

Router 2

```
R2#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.2
 Operational master IP address: 2.2.2.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 11 minutes 28 seconds (68800 centi sec)
 Skew time: 60 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: FALSE
```

Router 3

```
R3#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.3
 Operational master IP address: 2.2.2.1
 Priority is 254
```

```
Advertisement interval: 100 centi sec
Master Advertisement interval: 100 centi sec
Virtual router uptime: 0 hours 14 minutes 23 seconds (86300 centi sec)
Skew time: 0 centi sec
Accept mode: TRUE
Preempt mode: TRUE
Multicast membership on IPv4 interface eth2: JOINED
V2-Compatible: FALSE
```

Ping Output at Host A

```
HOSTA#ping 1.1.1.5
Press CTRL+C to exit
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=1.09 ms
```

Disabling the Master/Owner

`#configure terminal`	Enter the Configure mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#disable`	Disable the VRRP session.

Output After Disabling the Master

Router 1

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminDown - Init (admin state down)
 Virtual IP address: 2.2.2.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 0 seconds (0 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: LEFT
 V2-Compatible: FALSE
```

Router 3

```
R3#sh vrrp
VRRP Version: 3
```

```
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.3
 Operational master IP address: 2.2.2.3
 Priority is 254
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 40 minutes 55 seconds (245500 centi sec)
 Skew time: 0 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: FALSE

HOSTA#ping 1.1.1.5
Press CTRL+C to exit
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=1.09 m
```

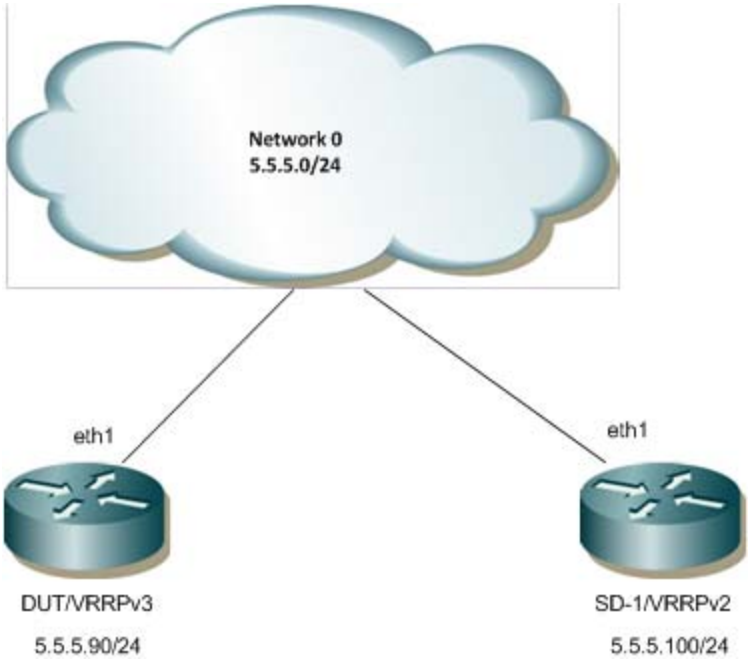
VRRP-Backward Compatibility

This section contains VRRP Backward Compatibility configuration examples.

The backward compatibility feature which implements version 3 of VRRP protocol recognizes the presence of VRRP version 2 compatible routers in the network and performs all operations normally. This support is intended for upgrade scenarios and is not recommended for permanent deployments. This should only occur when a router is transitioning from VRRPv2 to VRRPv3.

VRRP Backward Compatibility is applicable only for VRRP IPv4.

Topology



DUT

`#configure terminal`	Enter the Configure mode.
`(config)# interface eth1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.90/24`	Configure IP address on the interface.
`(config-if)#end`	Exit from configuration mode.
`#configure terminal`	Enter Configuration mode.
`(config)# router vrrp 1 eth1`	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface eth1.
`(config-router)#virtual-ip 5.5.5.190`	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
`(config-router)#enable`	Enable VRRP session on DUT.
`(config-router)#end`	Exit router VRRP mode.
`#configure terminal`	Enter Configuration mode.
`(config)#vrrp compatible-v2 enable`	Enable VRRP-Backward compatibility feature on a VRRPv3 running router.

SD-1

`#configure terminal`	Enter the Configure mode.
`(config)# interface eth1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.100/24`	Configure IP address on the interface.
`(config-if)#end`	Exit from configuration mode.
`#configure terminal`	Enter Configuration mode.

(config)#router vrrp 1 eth1	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface eth1.
(config-router)#virtual-ip 5.5.5.190	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
(config-router)#enable	Enable VRRP session on DUT.
(config-router)#end	Exit router VRRP mode.

Validation

DUT

```
#show vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.50
 Operational master IP address: 10.10.10.50
 Priority not configured; Current priority: 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 15 seconds (1500 centi sec)
 Skew time: 60 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Monitored circuit: eth1, Priority Delta: 20, Status: UP
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE
```

SD-1

```
#show vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.40
 Operational master IP address: 10.10.10.50
 Priority is 90
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 29 seconds (2900 centi sec)
 Skew time: 64 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
```

```
Multicast membership on IPv4 interface eth2: JOINED
V2-Compatible: FALSE
```

Redundancy Using VRRP and OSPF: Two Virtual Routers

This example illustrates a configuration of two routers between two end-hosts. R1 and R2 are two virtual routers functioning as backups for each other, with VRRP running on the 10.10.12.0/24 network (LAN), and OSPF running on the 10.10.10.0/24 network (ISP).

Topology

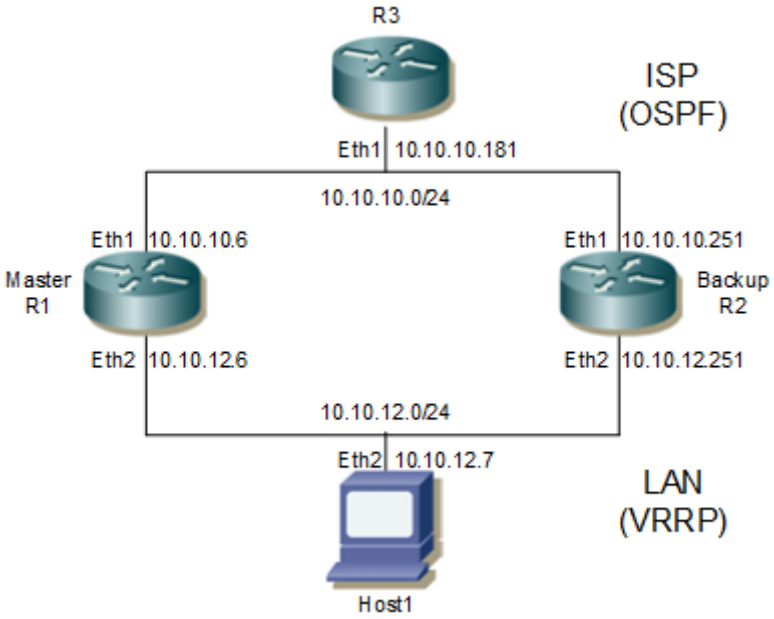


Figure 1-102: Redundancy Using VRRP and OSPF

In Figure 1-102:

- R3 is an OSPF router representing an OSPF network to an ISP.
- R1 is the VRRP Master/OSPF router.
- R2 is the VRRP Backup/OSPF router.
- Host 1 is an end-host.

VRRP handles any failure of the Master's link to the LAN. Failures in the OSPF network that could cause the Master to lose routing information would cause packets from Host 1 that are targeted for R3 to be dropped. Running VRRP on the OSPF network to create redundancy is undesirable, because doing so would cause erroneous VRRP packets to be sent to the ISP.

An alternative method to achieve redundancy is to run OSPF on the LAN side. By running OSPF on the LAN, any routing information lost by the Master would be regained from the Backup on the LAN interface, resulting in ICMP redirects to R2 for traffic received from Host 1. To reduce OSPF control traffic, R1 and R2 are configured as Area Border Routers (ABR), and the LAN is configured as a stub network to reduce LSA advertisement traffic on the LAN. Before enabling OSPF on the LAN, verify that VRRP is running with R1 as the Master and R2 as the Backup.

```
R1#show vrrp
 VrId <1>
```

```
 State is Master
 Virtual IP is 10.10.12.6 (IP owner)
 Interface is eth1
 Priority is 255
 Advertisement interval: 5 centi sec
 Preempt mode is TRUE
R2#show vrrp
 VrId <1>
  State is Backup
  Virtual IP is 10.10.12.6 (Not IP owner)
  Interface is eth1
  Priority is 100
  Advertisement interval: 5 centi sec
  Preempt mode is TRUE
```

Steps to configure OSPF on the LAN are given below.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (1). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.10.181`	Specify the OSPF router ID.
`(config-router)#timers spf exp 0 0`	Set `timers` to minimum time for quick convergence.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).

R1

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (1). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.12.6`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.10.12.0/24`) on which OSPF runs and associate the area ID (1)

R2

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the process ID (1). The process ID should be a unique integer
`(config-router)#ospf router-id 10.10.12.251`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.

`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (`0`).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.12.10.0/24`) on which OSPF runs and associate the area ID (`1`)

Verification

1. Set gateway on the end-host (statically):

```
(root@host1)#route add -net 10.10.10.0 netmask 255.255.255.0 gw 10.10.12.6
```

2. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.835 ms 0.350 ms 0.341 ms
2 10.10.10.181 (10.10.10.181) 9.557 ms 0.572 ms 0.545 ms
```

3. Bring down eth2 of R1:

```
[root@r1 sbin]#ifconfig eth2 down
```

4. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.461 ms 0.352 ms 0.334 ms
2 10.10.12.251 (10.10.12.251) 0.425 ms 0.432 ms 0.410 ms
3 10.10.10.181 (10.10.10.181) 0.691 ms 0.639 ms 0.607 ms
```

5. Bring up eth2 of R1:

```
[root@r1 sbin]#ifconfig eth2 up
```

6. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.457 ms 0.356 ms 0.443 ms
2 10.10.10.181 (10.10.10.181) 0.698 ms 0.642 ms 0.618 ms
```

VRRP Over MLAG

This section contains VRRP over MLAG configuration examples.

In this configuration TOR1 and TOR2 forms the VRRP master/backup relationship over MLAG interface.

Topology

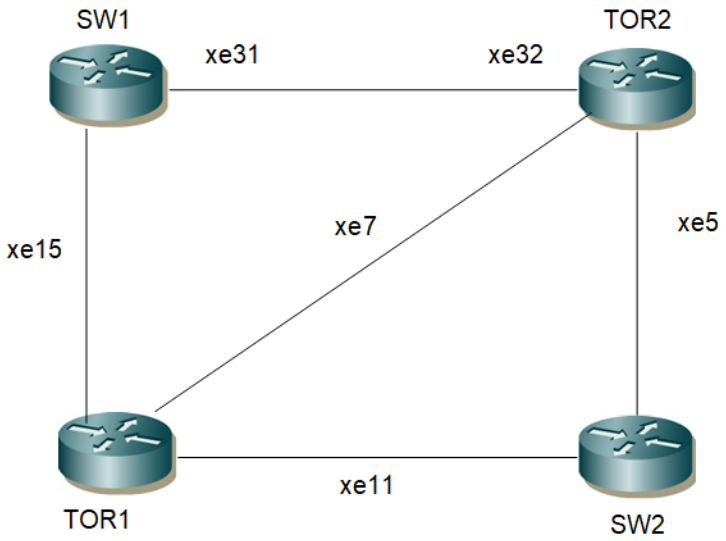


Figure 1-103: VRRP over MLAG

SW1

`#config terminal`	Enter the Configure mode.
`(config)#hostname SW1`	Assign the hostname for the router.
`SW1(config)# bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter to VLAN database
`SW1(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create VLANs
`SW1(config-vlan)#exit`	Exit the VLAN database mode
`SW1(config)# int po1`	Enter the interface mode
`SW1(config-if)#switchport`	Configure the interface as Layer 2
`SW1(config-if)# bridge-group 1`	Assign the bridge to the interface.
`SW1(config-if)#switchport mode trunk`	Configure the interface as trunk mode
`SW1(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN IDs
`SW1(config-if)#exit`	Exit the interface mode
`SW1(config)# int xe15`	Enter the interface mode
`SW1(config-if)# channel-group 1 mode active`	Add the interface as member of LAG interface

SW1(config-if)# int xe31	Enter the interface mode
SW1(config-if)# channel-group 1 mode active	Add the interface as member of LAG interface
SW1(config-if)# int xe36	Enter the interface mode
SW1(config-if)#switchport	Configure the interface as Layer 2
SW1(config-if)# bridge-group 1	Assign the bridge to the interface.
SW1(config-if)#switchport mode trunk	Configure the interface as trunk mode
SW1(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN IDs
SW1(config-if)#exit	Exit the interface mode

TOR1

#config terminal	Enter the Config terminal
(config)#hostname TOR1	Assign the hostname to the router
TOR1(config)# bridge 1 protocol rstp vlan-bridge	Configure the bridge
TOR1(config)#vlan database	Enter the VLAN database
TOR1(config-vlan)#vlan 2-1002 bridge 1 state enable	Configure VLANs
TOR1(config-vlan)#exit	Exit the VLAN database
TOR1(config)# int po1	Enter the interface mode
TOR1(config-if)#switchport	Configure the interface as L2
TOR1(config-if)# bridge-group 1	Assign the bridge to the interface
TOR1(config-if)#switchport mode trunk	Configure the interface as trunk mode
TOR1(config-if)#switchport trunk allowed vlan all	Configure to allow all the VLANs
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)# int xe15	Enter the interface mode
TOR1(config-if)# channel-group 1 mode active	Assign the interface as member of LAG interface
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#mcec domain configuration	Enter the MCEC mode
TOR1(config-mcec-domain)#domain-system-number 1	Assign the domain system number for MLAG interface.
TOR1(config-mcec-domain)#domain-address 1111.2222.3333	Assign the domain address
TOR1(config-mcec-domain)#domain-hello-timeout short	Assign the domain hello timeout
TOR1(config-mcec-domain)#intra-domain-link xe7	Assign the interface as IDL
TOR1(config-mcec-domain)#exit	Exit the MCEC domain
TOR1(config)#interface lo	Enter the interface mode
TOR1(config-if)#ip add 1.1.1.1/32 secondary	Create the MLAG interface.
TOR1(config-if)#int xe11	Exit the interface mode
TOR1(config-if)#ip add 20.20.20.1/24	Enter the interface mode

TOR1(config-if)#exit	Assign IP address to the interface
TOR1(config)#router ospf 100	Enter the interface mode
TOR1(config-router)#network 20.20.20.1/24 area 0	Assign IP address to the interface
TOR1(config-router)#network 1.1.1.1/32 area 0	Exit the interface mode
TOR1(config-router)#redistribute connected	Enter the OSPF router mode
TOR1(config-router)#exit	Add the network to the OSPF process
TOR1(config)#int po1	Add the network to the OSPF process
TOR1(config-if)#mlag 1	Redistribute the connected routes
TOR1(config-if)#exit	Exit the OSPF process
TOR1(config)#int vlan1.2	Enter interface mode
TOR1(config-if)#ip address 10.10.10.1/24	Assign IP address
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#router vrrp 1 vlan1.2	Create the VRRP process
TOR1(config-router)# virtual-ip 10.10.10.1 owner	Assign the virtual IP address to VRRP
TOR1(config-router)#enable	Enable the VRRP process
TOR1(config-router)#exit	Exit the VRRP mode
TOR1(config)#end	End the config terminal

TOR2

#config terminal	Enter the Config terminal
(config)#hostname TOR2	Assign the hostname to the router
TOR2(config)# bridge 1 protocol rstp vlan-bridge	Configure the bridge
TOR2(config)#vlan database	Enter the VLAN database
TOR2(config-vlan)#vlan 2-1002 bridge 1 state enable	Configure VLANs
TOR2(config-vlan)#exit	Exit the VLAN database
TOR2(config)# int po1	Enter the interface mode
TOR2(config-if)#switchport	Configure the interface as L2
TOR2(config-if)# bridge-group 1	Assign the bridge to the interface
TOR2(config-if)#switchport mode trunk	Configure the interface as trunk mode
TOR2(config-if)#switchport trunk allowed vlan add 2	Configure to add the VLAN 2 to the receiving packet.
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)# int xe32	Enter the interface mode
TOR2(config-if)# channel-group 1 mode active	Assign the interface as member of LAG interface
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#mcec domain configuration	Enter the MCEC mode
TOR2(config-mcec-domain)#domain-system-number 2	Assign the domain system number for MLAG interface.

TOR2(config-mcec-domain)#domain-address 1111.2222.3333	Assign the domain address
TOR2(config-mcec-domain)#domain-hello-timeout short	Assign the domain hello timeout
TOR2(config-mcec-domain)#intra-domain-link xe7	Assign the interface as IDL
TOR2(config-mcec-domain)#exit	Exit the MCEC domain
TOR2(config)# int po1	Enter the interface mode
TOR2(config-if)# mlag 1	Create the MLAG interface.
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface lo	Enter the interface mode
TOR2(config-if)#ip add 2.2.2.2/32 secondary	Assign IP address to the interface
TOR2(config-if)#int xe5	Enter the interface mode
TOR2(config-if)#ip add 30.30.30.1/24	Assign IP address to the interface
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#router ospf 100	Enter the OSPF router mode
TOR2(config-router)#network 30.30.30.1/24 area 0	Add the network to the OSPF process
TOR2(config-router)#network 2.2.2.2/32 area 0	Add the network to the OSPF process
TOR2(config-router)#redistribute connected	Redistribute the connected routes
TOR2(config-router)#exit	Exit the OSPF process
TOR2(config)#int vlan1.2	Enter interface mode
TOR2(config-if)#ip address 10.10.10.2/24	Assign IP address
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#router vrrp 1 vlan1.2	Create the VRRP process
TOR2(config-router)# virtual-ip 10.10.10.1	Assign the virtual IP address to VRRP
TOR2(config-router)#enable	Enable the VRRP process
TOR2(config-router)#exit	Exit the VRRP mode
TOR2(config)#end	End the config terminal

SW2

#config terminal	Enter the Config terminal
(config)#hostname SW2	Assign the hostname to the router
SW2(config)# bridge 1 protocol rstp vlan-bridge	Configure the bridge
SW2(config)#vlan database	Enter the VLAN database
SW2(config-vlan)#vlan 2-1002 bridge 1 state enable	Configure VLANs
SW2(config-vlan)#exit	Exit the VLAN database
SW2(config)# int xe11	Enter the interface mode
SW2(config-if)#ip address 20.20.20.2/24	Assign IP address to the interface
SW2(config-if)# int xe5	Enter the interface mode

SW2(config-if)#ip address 30.30.30.2/24	Assign IP address to the interface
SW2(config-if)# int xe46	Enter the interface mode
SW2(config-if)#ip address 40.40.40.1/24	Assign IP address to the interface
SW2(config-if)#int lo	Enter the interface mode
SW2(config-if)#ip add 3.3.3.3/32 secondary	Assign IP address to the interface
SW2(config-if)#int xe32	Enter the interface mode
SW2(config-if)#ip add 50.50.50.2/24	Assign IP address to the interface
SW2(config-if)#exit	Exit interface mode
SW2(config)# router ospf 100	Enter OSPF router
SW2(config-router)# network 3.3.3.3/32 area 0	Add the IP address to the OSPF process
SW2(config-router)# network 20.20.20.0/24 area 0	Add the IP address to the OSPF process
SW2(config-router)# network 30.30.30.0/24 area 0	Add the IP address to the OSPF process
SW2(config-router)#network 50.50.50.2/24 area 0	Add the IP address to the OSPF process
SW2(config-router)#exit	Exit the OSPF mode
SW2(config)#end	End the config mode.

Validation

TOR1

```
TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Total Bandwidth              : 10g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Active
  Switchover-mode              : Revertive
```

```
TOR1#show vrrp 1 vlan1.2
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.1
 Operational master IP address: 10.10.10.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 5 minutes 11 seconds (31100 centi sec)
 Master uptime: 0 hours 5 minutes 11 seconds (31100 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE
```

TOR2

```
TOR2#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Standby
  Switchover-mode               : Revertive

TOR2#show vrrp 1 vlan1.2
```

```
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.2
 Operational master IP address: 10.10.10.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 6 minutes 27 seconds (38700 centi sec)
 Skew time: 60 centi sec
 Master Down Interval: 360 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE
 Session is on MLAG interface. Dataplane acting as Master
```

CHAPTER 2 Interface Tracking

The need for VRRP Interface Tracking arose because VRRPv2 was unable to track the gateway interface status. The VRRP Interface Tracking feature provides dynamic failover of an entire circuit, in the event that one member of the group fails. It introduces the concept of a circuit, where two or more Virtual Routers on a single system can be grouped. In the event that a failure occurs, and one of the Virtual Routers performs the Master to Backup transition, the other Virtual Routers in the group are notified, and are forced into the Master to Backup transition, so that both incoming and outgoing packets are routed through the same gateway router, eliminating the problem for Firewall/NAT environments.

Note: Only 5 interfaces are supported in interface tracking for a VRRP session.

To configure VRRP Interface Tracking, each circuit is configured to have a corresponding priority-delta value, which is passed to VRRP when a failure occurs. The priority of each Virtual Router on the circuit is decremented by the priority-delta value, causing the VR Master to VR Backup transition.

In this example, two routers, R1 and R2, are configured as backup routers with different priorities. The priority-delta value is configured to be greater than the difference of both the priorities. R1 is configured to have a priority of 100, and R2 has a priority of 90. R1, with a greater priority, is the Virtual Router Master. The priority-delta value is 20, greater than 10 (100 minus 90). On R1, when the external interface `eth1` fails, the priority of R1 becomes 80 (100 minus 20). Since R2 has a greater priority (90) than R1, R2 becomes the VR Master, and routing of packages continues without interruption. When this VR Backup (R1) is up again, it regains its original priority (100), and becomes the VR Master again.

Topology

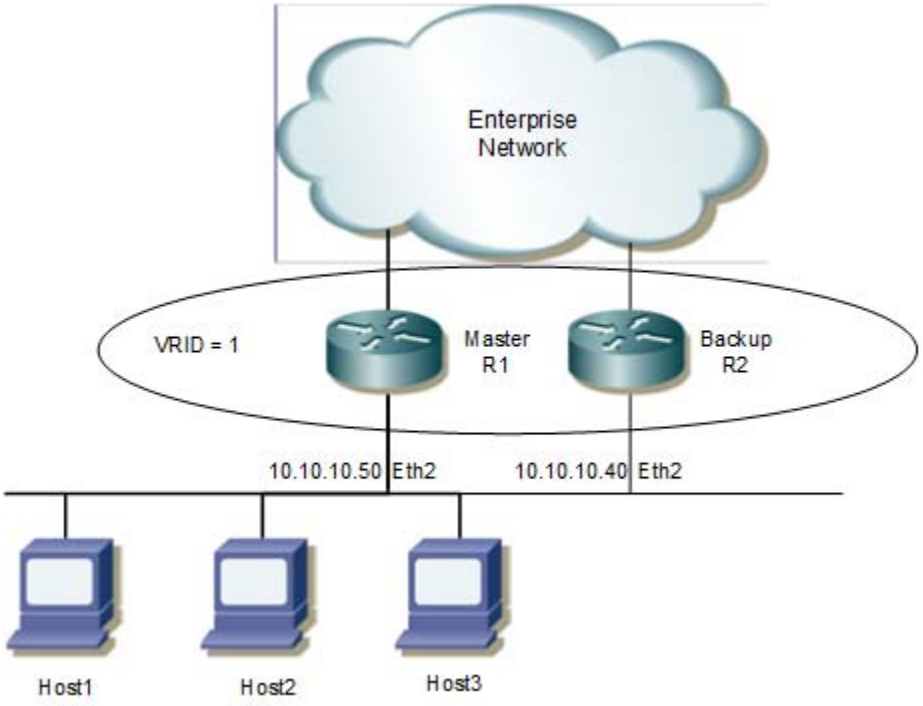


Figure 2-104: VRRP Interface Tracking

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a new VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.1`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 100`	Configure the priority to 100.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will own the external ip address when there is a failure.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#circuit-failover eth1 20`	Configure the priority-delta value to be 20. In case of failover, this priority-delta value is subtracted from the current VR Master.
`(config-router)#enable`	Enable the VRRP session on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a new VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.1`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 90`	Configure the priority to 90 (less than 100), because R2 is the VR Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a primary backup router in case of failure.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session on the router.

Validation

show vrrp

Virtual Router Redundancy Protocol Command Reference

Contents

This document contains these chapters:

CHAPTER 1 VRRP Commands

This chapter describes the commands for VRRP.

accept-mode

Use this command to enable/disable accept mode for the session.

Controls whether a VRRP master node will accept/respond to packets addressed to the Virtual-IP address as its own address if it is not the Virtual-IP Owner.

Command Syntax

```
accept-mode true
accept-mode false
```

Parameter

`true`	The accept-mode for the session is enabled.
`false`	The accept-mode for the session is disabled.

Default

By default, accept-mode for the session is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to set and unset the accept-mode.

```
#configure terminal
(config)#router vrrp 2 eth2
(config-router)#accept-mode false

# configure terminal
(config)#router vrrp 2 eth2
(config-router)#accept-mode True
```

advertisement-interval

Use this command to configure the advertisement interval of a virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s). The master virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the master virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the multicast address assigned to the VRRP group (224.0.0.18). Advertisements are sent every second by default.

Note: Higher-priority master routers with slower transmission rates than their backup routers are unstable. This is because low-priority nodes configured to faster rates could come online and decide they should be masters before they have heard anything from the higher-priority master with a slower rate. When this happens, it is temporary: once the lower-priority node does hear from the higher-priority Mmaster, it will relinquish mastership.

Use the no parameter with this command to restore the default setting.

Command Syntax

```
advertisement-interval <5-4095>
no advertisement-interval
```

Parameter

<5-4095>	Specify the advertisement interval in centi-seconds (in multiples of 5) when VRRPv3 is enabled

Default

By default, advertisements are sent every second

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to configure an advertisement interval of 50 centi-seconds for the virtual router with VR ID 2 on interface eth0.

```
#configure terminal
(config)#router ip vrrp 2 eth0
(config-router)#advertisement-interval 50
```

circuit-failover

Use this command to enable the VRRP circuit failover feature.

Use the no parameter with this command to disable this feature.

Command Syntax

```
circuit-failover [IFNAME] |<1-253>
no circuit-failover [IFNAME] |<1-253>
```

Parameters

IFNAME	Specify an interface of the router that is monitored by the virtual router. This is usually an upstream interface. Should the interface go down, another router, configured as backup within the VRRP group, may take over as a master.
<1-253>	Specify the delta value. The value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.

Default

By default, circuit failover feature is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to configure circuit failover for the VRRP session with VR ID 1. Interface eth1 is considered the monitored interface.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#circuit-failover eth1 30
```

debug vrrp

Use this command to specify debugging options for VRRP.

Use the no parameter with this command to disable debugging.

Command Syntax

```
debug vrrp (all|event|packet [send|recv|])
no debug vrrp (all|event|packet [send|recv|])
```

Parameters

all	Specify debugging options for all VRRP events.
event	Specify debugging options for VRRP event troubleshooting.
packet	Specify debugging options for VRRP packets
send	Specify the debug option set for sent packets.
recv	Specify the debug option set for received packets.

Command Mode

Configure mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to enable all VRRP debug options.

```
#configure terminal
(config)#debug vrrp all
```

The example below shows how to enable debugging options for VRRP events.

```
#configure terminal
(config)#debug vrrp events
```

The example below shows how to enable debug options for VRRP packets sent.

```
#configure terminal
(config)#debug vrrp packet send
```

The example below shows how to enable debug options for VRRP packets received.

```
#configure terminal
(config)#debug vrrp packet recv
```

disable

Use this command to disable a VRRP session on the router (to stop the router from participating in virtual routing). When this command is configured, a backup Router assumes the Role of Master depending on its priority.

Command Syntax

```
disable
```

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to disable a VRRP session.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#disable
```

enable

Use this command to enable a VRRP session on the router (to make it participate in virtual routing). To make any changes to the VRRP configuration, first disable the router from participating in virtual routing using the `disable` command.

Note: Configure the virtual IP address and define an interface for the VRRP session (using the `virtual-ip` and `interface` commands) before using this command.

Command Syntax

```
enable
```

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to enable a VRRP session with VR ID 1 on interface eth0.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#enable
```

ipv4-exclude-pseudo-header

Use this command to exclude the pseudo-header in IPv4 VRRPv3 checksum calculation on the VRRP group in router mode to support IPv4 VRRPv3 interoperability.

Note: Use this command when checksum errors are observed with other vendors for VRRPv3.

Use the no form of this command to delete the VRRP IPv4 checksum pseudo-header exclude configuration from the VRRP group on the router.

Command Syntax

```
ipv4-exclude-pseudo-header
```

Parameter

None

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced in OcNOS-SP version 2.4.

Examples

```
#configure terminal
(config)#router vrrp 2 eth2
(config-router)#ipv4-exclude-pseudo-header

#configure terminal
(config)#router vrrp 2 eth2
(config-router)#no ipv4-exclude-pseudo-header
```

ip pim redundancy

Use this command to set the priority for which a router is elected as the designated router (DR).

Note: This command should be applied to the all related VRRP routers with identical priority values.

Command Syntax

```
ip pim redundancy <1-255> vrrp dr-priority <0-4294967294>
```

Parameter

`<1-255>`	VRRP virtual router identifier
`<0-4294967294>`	DR priority

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
OcNOS(config-if)#ip pim redundancy 1 vrrp dr-priority 900
OcNOS(config-if)#
```

operational-ip

Use this command to set the primary IPv4 address.

Use the no parameter with this command to remove a primary IPv4 address.

Command Syntax

```
operational-ip A.B.C.D
no operational-ip
```

Parameters

A.B.C.D	IPv4 address.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#operational-ip 1.2.3.4
```

preempt-mode

Use this command to configure preempt mode. If set to `true`, the highest priority backup is always the master when the default master is unavailable. If set to `false`, a higher priority backup does not preempt a lower priority backup which is acting as master.

When the master router fails, the backup routers come online in priority order — highest to lowest. Preempt mode set to `true` allows a higher priority backup router to relieve a lower priority backup.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. This preemptive scheme can be disabled using the `preempt-mode false` command. If preemption is disabled, the backup virtual router that is currently elected as Master does not transition to backup again when the alternate backup router with higher priority becomes available.

Command Syntax

```
preempt-mode (true|false)
```

Parameters

`true`	Specify that preemption is enabled.
`false`	Specify that preemption is disabled.

Default

By default, preempt mode is true

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to enable the preempt mode.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode false

#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode true
```

router vrrp

Use this command to enable a VRRP routing process.

Use the no form of this command to disable a VRRP routing process.

Command Syntax

```
router vrrp <1-255> IFNAME
no router vrrp <1-255> IFNAME
```

Parameters

<1-255>	Virtual router identifier
IFNAME	Interface name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
```

show debugging vrrp

Use this command to display the set VRRP debugging option.

Command Syntax

```
show debugging vrrp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging vrrp
VVRRP debugging status:
VRRP event debugging is on
VRRP packet debugging is on
```

show running-config vrrpv6

Use this command to show the running configuration for VRRPv6.

Command Syntax

```
show running-config router vrrpv6
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show running-config vrrpv6
!
vrrp vmac disable
!
!
router ipv6 vrrp 1 eth1
virtual-ipv6 fe80::c0
enable
!
```

show running-config router vrrp

Use this command to show the running configuration for VRRP.

Command Syntax

```
show running-config router vrrp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows the running configuration of VRRP. Virtual Router is configured as Master and Owner of IP address.

```
#show running-config router vrrp
!
router vrrp 1 eth0
 virtual-ip 39.0.0.24 owner
 advertisement-interval 5
 preempt-mode false
 enable
!
```

show vrrp

Use this command to display a list of virtual router identifiers that are configured on the router.

Command Syntax

```
show vrrp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vrrp

R1#show vrrp
VrId <1>
State is Master
Virtual IP is 10.10.12.6 (IP owner)
Interface is eth0
Priority is 255
Advertisement interval: 5 centi sec
Preempt mode is TRUE

R2#show vrrp
VrId <1>
State is Backup
Virtual IP is 10.10.12.6 (Not IP owner)
Interface is eth0
Priority is 100
Advertisement interval: 5 centi sec
Preempt mode is TRUE
```

Table 1-66 Explains the show command output fields.

Table 1-66: show vrrp output fields

Field	Description
VrID	Type of vr identifier by the system on the interface.
State	VRRP State: Master — The interface is acting as the master router interface. Backup —The interface is acting as the backup router interface.
Virtual IP	List of virtual IP addresses configured on the interface.
Interface	Name of the logical interface.

Field	Description
Priority	Configured VRRP priority for the interface.
Advertisement interval	Configured VRRP advertisement interval.
Preempt mode	Whether preemption is allowed on the interface.

show vrrp <1-255>

Use this command to display VRRP information for a virtual router.

Command Syntax

```
show vrrp <1-255> IFNAME
```

Parameters

<1-255>	Virtual router identifier
IFNAME	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vrrp 7 eth0
```

show vrrp (global | ipv4) statistics

Use this command to display VRRP global or ipv4 router statistics.

Command Syntax

```
show vrrp (global | ipv4 ) statistics
```

Parameters

`global`	Global (VRRP Router)
`ipv4`	VRRP IPv4 router

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8.

Example

```
#show vrrp global statistics
VRRP Global Statistics
Checksum Errors  : 0
Version Errors   : 0
VRid Errors      : 0
Discontinuity Time: 00 hour, 00 min, 00 sec


#show vrrp ipv4 statistics
Address family IPv4
VRRP Id: 1 on interface: xe1
Master Transitions: 0
Advertisements Rcvd: 0
Pkts Rcvd with IP TTL Errors: 0
Pkts Rcvd with Zero Priority: 0
Pkts Sent with Zero Priority: 0
Pkts Rcvd with Invalid TYPE: 0
Pkts Rcvd with Packet Length Errors: 0
Pkts Rcvd with IP Count Mismatch: 0
Discontinuity Time: 00 hour, 00 min, 00 sec
Refresh Rate: 1000 ms
```

snmp restart vrrp

Use this command to restart SNMP in Virtual Routing Redundancy Protocol (VRRP).

Command Syntax

```
snmp restart vrrp
```

Parameters

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart vrrp
```

switch-back-delay

Use this command to set a switch-back delay timer for the master VRRP router. This feature prevents the original master VRRP router from transitioning back to the master state after coming back online until the configured delay timer has expired.

Command Syntax

```
switch-back-delay <1-500000>
no switch-back-delay
```

Parameters

<1-500000>	Specify a switch-back delay in milliseconds.

Command Mode

Router mode

Default

By default, the switch-back delay is set to 0

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to set a switch-back delay timer of 7000 milliseconds.

```
#configure terminal
(config)#router vrrp 5 eth1
(config-router)#switch-back-delay 7000
```

undebug vrrp

Use this command to disable debugging options for VRRP.

Command Syntax

```
undebug vrrp (all|event|packet [send|recv|])
no undebug vrrp (all|event|packet [send|recv|])
```

Parameters

`all`	Specify debugging options for all VRRP events.
`event`	Specify debugging options for VRRP event troubleshooting.
`packet`	Specify debugging options for VRRP packets
`send`	Specify the debug option set for sent packets.
`recv`	Specify the debug option set for received packets.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#undebug vrrp all
```

The example below shows how to disable debug options for VRRP events.

```
#undebug vrrp events
```

The example below shows how to disable debug options for VRRP packets sent.

```
#undebug vrrp packet send
```

The example below shows how to disable debug options for VRRP packets received.

```
#undebug vrrp packet recv
```

virtual-ip

Use this command to set the virtual IP address for the VRRP virtual router as VRRP Owner. This is the IP address used by end hosts to address their default gateway.

The VRRP Owner of the Virtual IP address only responds to packets destined to the Virtual IP address (for example, ICMP packets destined to the Virtual IP address).

Use the `no` parameter with this command to remove a virtual IP address assignment.

Syntax Description

```
virtual-ip A.B.C.D (owner|)
no virtual-ip
```

Parameters

`A.B.C.D`	Specify the virtual IP address of the interface that participates in virtual routing.
`owner`	Specify the IP address as the owner.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to configure the router as VRRP owner.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#virtual-ip 10.10.20.30 owner
```

The example below removes the virtual IP address assignment.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#no virtual-ip
```

vrrp compatible-v2

Use this command to enable the backward-compatibility feature. When enabled, both VRRPv3 and VRRPv2 inter-operation are supported.

Command Syntax

```
vrrp compatible-v2 (enable| disable)
```

Parameters

`enable`	Enable VRRPv2 inter-operation
`disable`	Disable VRRPv2 inter-operation

Default

By default, vrrp compatible-v2 is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vrrp compatible-v2 enable
```

vrrp ipv4-exclude-pseudo-header

Use this command to excludes the pseudo-header in IPv4 VRRPv3 checksum calculation on the VRRP groups in configuration mode to support IPv4 VRRPv3 interoperability.

Note: Use this command when checksum errors are observed with other vendors for VRRPv3.

Command Syntax

```
vrrp ipv4-exclude-pseudo-header (enable| disable)
```

Parameters

`enable`	Enable ipv4-exclude-pseudo-header
`disable`	Disable ipv4-exclude-pseudo-header

Default

By default, VRRP includes the pseudo header in checksum calculation.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 2.4.

Examples

```
#configure terminal
(config)#vrrp ipv4-exclude-pseudo-header enable

#configure terminal
(config)#vrrp ipv4-exclude-pseudo-header disable
```

vrrp vmac

Use this command to enable or disable Virtual MAC (VMAC).

This command affects all VRRP groups in a router. On a single network segment, multiple VRRP groups can be configured, each using a different VMAC. The use of VMAC addressing allows for faster switchover when a backup router assumes the master role. When this command is used to enable a VMAC, the virtual router forwards packets with a special-purpose multicast VMAC address (0:0:5e:0:01:<VR ID>). Otherwise, it forwards with is interface's physical address.

The VMAC address is assigned to a router interface at the time the VRRP group is enabled in the router.

Command Syntax

```
vrrp vmac (enable|disable)
```

Parameters

`enable`	Enable virtual MAC addressing.
`disable`	Disable virtual MAC addressing and use physical MAC addressing.

Default

By default, VMAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to enable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac enable
```

The example below shows how to disable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac disable
```

SECTION 11 Bidirectional Forwarding Detection

Bidirectional Forwarding Detection Configuration Guide

Contents

This document contains these chapters and appendices:

CHAPTER 1 Base BFD Configuration

This chapter provides the steps for configuring the base Bidirectional Forwarding Detection (BFD) setup.

Overview

This section provides an overview of Bidirectional Forwarding Detection (BFD). BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols like BGP, EIGRP, IS-IS, and OSPF. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.The configuration and command reference for BFD is given in the following chapters in this section.

Topology

Figure 1-105: Basic Topology of Three Routers

BFD Echo Function

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd echo`	Enable BFD echo mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd echo`	Enable BFD echo mode.

Validation

R1

```
#sh bfd session detail

Session Interface Index : 3             Session Index : 1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Down
Local Discriminator : 1                 Local Address : 10.1.1.1/32
Remote Discriminator : 1                Remote Address : 10.1.1.2/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:01
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000010a               Pkt Out : 00000000000001f7
Echo Out : 00000000000000ab             IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000          IPv6 Pkt Out : 0000000000000000
UP Count : 57                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
#sh bfd session detail

Session Interface Index : 3             Session Index : 1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                 Local Address : 10.1.1.2/32
Remote Discriminator : 1                Remote Address : 10.1.1.1/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 1000
```

```
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000ad                Pkt Out : 0000000000000105
Echo Out : 0000000000000063              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 33                            UPTIME : 00:00:03

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Slow Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

BFD Multihop Peer Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 20.1.1.3 interval 100 minrx 100 multiplier 3`	Configure BFD `multihop-peer` timer and reception intervals in milliseconds and the Hello multiplier.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#interface eth2`	Enter interface Mode.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#router ospf 1`	Enter router OSPF mode
`R2(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#redistribute connected`	
`R2(config-router)#exit`	Exit router OSPF mode

R3

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth2`	Enter interface Mode.
`R1(config-if)#ip address 20.1.1.3/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 10.1.1.1 interval 100 minrx 100 multiplier 3`	Configure BFD `multihop-peer` timer and reception intervals in milliseconds and the Hello multiplier.

Validation:

R1

```
#sh bfd session detail


Session Interface Index : 0              Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 2                  Local Address : 10.1.1.1/32
Remote Discriminator : 0                 Remote Address : 20.1.1.3/32
Local Port : 49153                       Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100               Min Rx: 100               Multiplier: 3
Neg Tx: 0                 Neg Rx: 0                 Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000000                Pkt Out : 0000000000000097
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 0                             UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R3

```
#sh bfd session detail


Session Interface Index : 0              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 1                  Local Address : 20.1.1.3/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100               Min Rx: 100               Multiplier: 3
Neg Tx: 100               Neg Rx: 100               Neg detect mult: 3
```

```
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001df                Pkt Out : 00000000000001e0
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:01:26

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Single-hop Session Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R1(config-if)#exit`	Exit from interface mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R2(config-if)#exit`	Exit from interface mode.

Validation:

R1

```
#sh bfd session detail

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
```

```
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100              Min Rx: 100             Multiplier: 4
Neg Tx: 100              Neg Rx: 100             Neg detect mult: 4
Min echo Tx: 100         Min echo Rx: 1000       Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000156e                Pkt Out : 0000000000001748
Echo Out : 000000000000019b              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 139                           UPTIME : 00:14:23

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
#sh bfd session detail

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100              Min Rx: 100             Multiplier: 4
Neg Tx: 100              Neg Rx: 100             Neg detect mult: 4
Min echo Tx: 100         Min echo Rx: 1000       Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000181d                 Pkt Out : 00000000000019ab
Echo Out : 00000000000001b5              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
```

```
    UP Count : 145                          UPTIME : 00:15:19

    Protocol Client Info:
    BFD-> Client ID: 28      Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    1
```

BFD Echo Interval

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#bfd echo interval 100`	.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd echo`	Enable BFD echo mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R1(config-if)#bfd echo interval 100`	.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd echo`	Enable BFD echo mode.

Validation

R1

```
    #sh bfd session detail

    Session Interface Index : 3             Session Index : 1
    Lower Layer : IPv4                      Version : 1
    Session Type : Single Hop               Session State : Down
    Local Discriminator : 1                 Local Address : 10.1.1.1/32
    Remote Discriminator : 1                Remote Address : 10.1.1.2/32
    Local Port : 49152                      Remote Port : 3784
    Local Echo Port : 49153
    Options :
    Echo Enabled
    Diagnostics : None

    Timers in Milliseconds :
```

```
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001ea                Pkt Out : 0000000000000398
Echo Out : 0000000000000147              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 109                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
#sh bfd session detail

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Down
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:01
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000028f                Pkt Out : 00000000000003b8
Echo Out : 0000000000000183              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 129                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

CHAPTER 2 BFD Protocol Configurations

This chapter describes the BFD protocol configurations.

OSPF—BFD Single-Hop Session

This section provides the steps for configuring BFD for Single-Hop OSPF.

Topology

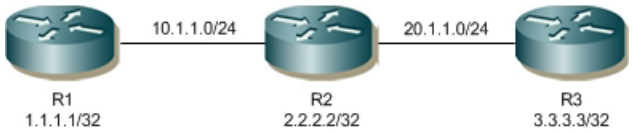


Figure 2-106: Single-Hop OSPF Topology

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface lo`	Enter the Interface configuration mode for lo
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Assign IP Address
`R1(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP Address
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.
`R1(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R1(config-router)#network 1.1.1.1/32 area 1`	Advertise loopback network `1.1.1.1/32` in OSPF `area 1`.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
`R1(config-router)#exit`	Exit the router mode

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode
`R2(config)#router ospf 100`	Enter the Router mode for OSPF.
`R2(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.

R2(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R2(config-router)#network 2.2.2.2/32 area 1	Advertise loopback network 2.2.2.2/32 in OSPF area 1.
R2(config-router)#bfd all-interfaces	Enable BFD for all neighbors.
R2(config)#interface lo	Enter the Interface configuration mode for lo
R2(config-if)#ip address 2.2.2.2/32 secondary	Assign IP Address
R2(config-router)#exit	Exit the router mode.

R3

R3#configure terminal	Enter the Configure mode.
R3(config)#interface lo	Enter the Interface configuration mode for lo
R3(config-if)#ip address 3.3.3.3/32 secondary	Assign IP Address
R3(config)#interface eth2	Enter the Interface configuration mode for eth2.
R3(config-if)#ip address 20.1.1.2/24	Assign IP Address.
R3(config-if)#exit	Exit the Interface configuration mode.
R3(config)#router ospf 100	Enter the Router mode for OSPF.
R3(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R3(config-router)#network 3.3.3.3/32 area 1	Advertise loopback network 3.3.3.3/32 in OSPF area 1.
R3(config-router)#bfd all-interfaces	Enable BFD for all neighbors
R3(config-router)#exit	Exit the router mode.

Validation

R1

```
R1#show ip ospf n

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1   Full/Backup      00:00:35    10.1.1.2           xe23          0


R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface  Down-
Reason  Remote-Addr
1                   1             IPv4        Single-Hop     Up         00:02:55
xe23       NA                   10.1.1.2/32
257                 0             IPv4        Multi-Hop      Up          00:00:18
xe8         NA                   3.3.3.3/32
Number of Sessions:    2
```

```
R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10023          Interface name :xe23
Session Index : 1
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                  Session State : Up
Local Discriminator : 1                       Local Address : 10.1.1.1/32
Remote Discriminator : 1                   Remote Address : 10.1.1.2/32
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000814                Pkt Out : 00000000000000000814
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:59

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                  Session Index : 257
Lower Layer : IPv4                              Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                     Local Address : 1.1.1.1/32
Remote Discriminator : 0                   Remote Address : 3.3.3.3/32
Local Port : 49153                              Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
```

```
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 0                        Neg Rx: 0                        Neg detect mult: 0
Min echo Tx: 1000          Min echo Rx: 1000          Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                Pkt Out : 00000000000000000107
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00
R3#show bfd session
BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface    Down-Reason
Remote-Addr
1          1      IPv4       Single-Hop   Up     00:04:33   eth2           NA
20.1.1.3/32
--------------------------------------------------------------------------------

R1#show bfd session detail
======================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000cf3                Pkt Out : 0000000000000cfc
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
```



```
UP Count : 1                              UPTIME : 00:12:12

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1

R2#show bfd session detail
============================================================

Session Interface Index : 3
Interface name : eth1                     Session Index : 1
Lower Layer : IPv4                        Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 1                   Local Address : 10.1.1.2/32
Remote Discriminator : 1                  Remote Address : 10.1.1.1/32
Local Port : 49152                        Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000d6f                 Pkt Out : 0000000000000da5
Echo Out : 0000000000000000               IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000            IPv6 Pkt Out : 0000000000000000
UP Count : 1                              UPTIME : 00:12:39

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------

Session Interface Index : 4
Interface name : eth1                     Session Index : 2
Lower Layer : IPv4                        Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 2                   Local Address : 20.1.1.1/32
Remote Discriminator : 1                  Remote Address : 20.1.1.2/32
Local Port : 49153                        Remote Port : 3784
Options :

Diagnostics : None
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000d30                Pkt Out : 0000000000000d5e
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:24
```

R2

```
R2#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface  Instance ID
1.1.1.1           1   Full/DR          00:00:32      10.1.1.1           xe9/3       0
3.3.3.3           1   Full/Backup    00:00:40     20.1.1.2           xe17/1     0


R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1               1               IPv4            Single-Hop    Up         00:02:33
xe9/3           NA          10.1.1.1/32
2               1               IPv4            Single-Hop    Up         00:01:54
xe17/1          NA          20.1.1.2/32
Number of Sessions:    2


R2#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10023          Interface name :xe9/3
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
```

```
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000713                 Pkt Out : 00000000000000000714
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:37

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 10053          Interface name :xe17/1
Session Index : 2
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                     Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32
Local Port : 49153                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                    Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000535              Pkt Out : 00000000000000000537
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
```

```
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:58

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

R3

```
R3#show ip ospf n

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1     Full/DR         00:00:36    20.1.1.1          xe17/10       0


R3#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1                    2          IPv4            Single-Hop      Up         00:01:21
xe17/1             NA           20.1.1.1/32
257                    1           IPv4              Multi-Hop             Up
00:00:00      xe6                NA           1.1.1.1/32
Number of Sessions:    2
Total number of Established sessions 2


R3#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10053         Interface name :xe17/1
Session Index : 1
Lower Layer : IPv4                           Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                    Local Address : 20.1.1.2/32
Remote Discriminator : 2                Remote Address : 20.1.1.1/32
Local Port : 49152                           Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                  Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                  Neg detect mult: 3
```

```
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000391                  Pkt Out : 00000000000000000391
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:01:26

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                  Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                       Local Address : 3.3.3.3/32
Remote Discriminator : 1                       Remote Address : 1.1.1.1/32
Local Port : 49153                                  Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                         Min Rx: 250                    Multiplier: 3
Neg Tx: 250                         Neg Rx: 250                    Neg detect mult:250
Min echo Tx: 1000              Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                  Pkt Out : 00000000000000000047
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

OSPF—BFD Multi-Hop Session

This section provides the steps for configuring BFD for OSPF multi-hop sessions.

Topology

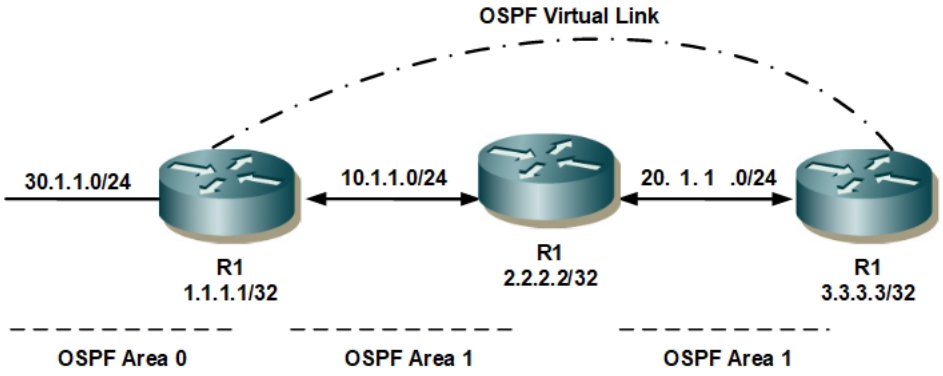


Figure 2-107: Multi-hop OSPFv2 Topology

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface lo`	Enter the Interface configuration mode for lo
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Assign IP Address
`R1(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP Address
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)#interface eth2`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 30.1.1.1/24`	Assign IP Address
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.
`R1(config-router)#ospf router-id 1.1.1.1`	OSPF router ID in IPv4 format
`R1(config-router)#network 10.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R1(config-router)#network 1.1.1.1/32 area 1`	Advertise loopback network `1.1.1.1/32` in OSPF `area 1.`
`R1(config-router)#network 30.1.1.0/24 area 0`	Advertise network `30.1.1.0/24` in OSPF `area 0`.
`R1(config-router)#area 1 virtual-link 3.3.3.3 fall-over bfd`	Create a virtual link to R3 with BFD.

R2

`R2#configure terminal`	Enter the Configure mode
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.

`R2(config-if)#ip address 10.1.1.2/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode
`R2(config)#interface lo`	Enter the Interface configuration mode for lo
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode
`R2(config)#router ospf 100`	Enter the Router mode for OSPF.
`R2(config-router)#ospf router-id 2.2.2.2`	OSPF router ID in IPv4 format
`R2(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R2(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R2(config-router)#network 2.2.2.2/32 area 1`	Advertise loopback network `2.2.2.2/32` in OSPF `area 1`.
`R2(config-router)#exit`	Exit the router mode.

R3

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#interface lo`	Enter the Interface configuration mode for lo
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Assign IP Address
`R3(config-if)#exit`	Exit the Interface configuration mode.
`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 20.1.1.2/24`	Assign IP Address.
`R3(config-if)#exit`	Exit the Interface configuration mode.
`R3(config)#router ospf 100`	Enter the Router mode for OSPF.
`R3(config-router)#ospf router-id 3.3.3.3`	OSPF router ID in IPv4 format
`R3(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R3(config-router)#network 3.3.3.3/32 area 1`	Advertise loopback network `3.3.3.3/32` in OSPF `area 1`.
`R3(config-router)#area 1 virtual-link 1.1.1.1 fall-over bfd`	Create a virtual link to R1 with BFD.

Validation

```
R1#sh bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
257           257              IPv4       Multi-Hop       Up        00:00:54
NA         NA                   20.1.1.2/32
```

```
Number of Sessions:    1


R2#sh bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
Number of Sessions:    0



R3#sh bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
257        257          IPv4         Multi-Hop   Up          00:01:46  NA        NA
10.1.1.1/32

Number of Sessions:    1


R1#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 0              Session Index : 257
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                Local Address : 10.1.1.1/32
Remote Discriminator : 257               Remote Address : 20.1.1.2/32
Local Port : 49152                       Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled
```

```
Counters values:
Pkt In : 00000000000000000606                Pkt Out : 00000000000000000605
Pkts Drop : 00000000000000000000             Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000              IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                 UPTIME : 00:02:13

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1



R2#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
Number of Sessions:    0
R2#


R3#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 0              Session Index : 257
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                Local Address : 20.1.1.2/32
Remote Discriminator : 257               Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000529                Pkt Out : 00000000000000000530
Pkts Drop : 00000000000000000000             Auth Pkts Drop : 00000000000000000000
```

```
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:56

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Configuration in IS-IS

This section provides the steps for configuring BFD for the IS-IS protocol.

Topology

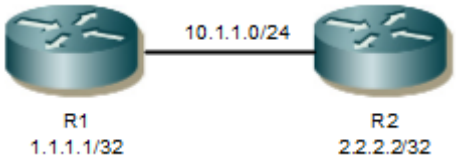


Figure 2-108: Basic Topology for BFD-ISIS

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IP address.
`R2(config-if)#ip router isis 1`	Configure ISIS router
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#router isis 1`	Enter the Router mode for IS-IS.
`R1(config-router)#net 10.0000.0000.0001.00`	Advertise network `10.0000.0000.0001.00` in IS-IS.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface mode.
`R2(config-if)#ip address 10.1.1.2/24`	Configure IP address.
`R2(config-if)#ip router isis 1`	Configure ISIS router
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#router isis 1`	Enter the Router mode for IS-IS.
`R2(config-router)#net 10.0000.0000.0002.00`	Advertise network `10.0000.0000.0002.00` in IS-IS.
`R2(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.

Validation

```
R1#show bfd session

    BFD process for VRF: (DEFAULT VRF)
    ========================================================================
    =======
    Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
    Down-Reason Remote-Addr
    1                    1           IPv4             Single-Hop      Up
    00:00:42      eth1           NA                     10.1.1.1/32

    Number of Sessions:    1

    R2#show bfd session

    BFD process for VRF: (DEFAULT VRF)
    ========================================================================
    =======
    Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
    Down-Reason  Remote-Addr
    1            1            IPv4    Single-Hop  Up  00:10:23      eth1
    NA       10.1.1.2/32
    1            1            IPv4    Single-Hop  Up  00:10:23      eth2
    NA       20.1.1.2/32
    Number of Sessions:    2

R1#show bfd session detail
=======================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 10.1.1.1/32
Remote Discriminator : 3                 Remote Address : 10.1.1.2/32
Local Port : 49153                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 2000             Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000027b                Pkt Out : 0000000000000278
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
```

```
UP Count : 1                              UPTIME : 00:02:19

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
-------------------------------------------------------
Number of Sessions:    1

R2#sh bfd session detail
=======================================================

Session Interface Index : 3
Interface name : eth1                     Session Index : 3
Lower Layer : IPv4                        Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 3                   Local Address : 10.1.1.2/32
Remote Discriminator : 2                  Remote Address : 10.1.1.1/32
Local Port : 49154                        Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250              Multiplier: 3
Neg Tx: 250               Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000002db                 Pkt Out : 00000000000002dd
Echo Out : 0000000000000000               IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000            IPv6 Pkt Out : 0000000000000000
UP Count : 1                              UPTIME : 00:02:42

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
-------------------------------------------------------
Number of Sessions:    1
```

BFD Configuration in BGP

This section provides the steps for configuring BFD for the BGP protocol.

Topology

Figure 2-109: Basic Topology for BFD in BGP

R1

`R1#configure terminal`	Enter configure mode
`R1(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP Address
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)# interface lo`	Enter interface mode
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Configure the IP address on loopback interface.
`R1(config-if)#bfd session 1.1.1.1 3.3.3.3 multihop`	Enable BFD multihop session
`R1(config)#router ospf 100`	Enter Router mode for OSPF
`R1(config-router)# ospf router-id 1.1.1.1`	Configure router-id in OSPF
`R1(config-router)# network 1.1.1.1/32 area 0.0.0.1`	Advertise network 1.1.1.1/32 in OSPF area 1.
`R1(config-router)# network 10.1.1.0/24 area 0.0.0.1`	Advertise network 10.1.1.0/24 in OSPF area 1.
`R1(config)#router bgp 100`	Enter Router mode for BGP
`R1(config-router)# neighbor 3.3.3.3 remote-as 100`	Add the neighbor 3.3.3.3 to remote-as 100.
`R1(config-router)# neighbor 3.3.3.3 fall-over bfd`	Enable BFD option for neighbor `multihop`
`R1(config-router)#neighbor 3.3.3.3 update-source lo`	Add neighbor 3.3.3.3 to update-source lo.
`R1(config-router)#neighbor 10.1.1.2 remote-as 100`	Add neighbor 10.1.1.2 to remote-as 100.
`R1(config-router)# neighbor 10.1.1.2 fall-over bfd`	Enable BFD option for neighbor
`R1(config-router)#end`	Exit from Router BGP mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP Address

R2(config-if)#exit	Exit the Interface configuration mode
R2(config)# interface lo	Enter interface mode
R2(config-if)#ip address 2.2.2.2/32 secondary	Configure the IP address on loopback interface.
R2(config-if)#exit	Exit the Interface configuration mode
R2(config)#router ospf 100	Enter Router mode for OSPF
R2(config-router)#ospf router-id 2.2.2.2	Configure router-id in OSPF
R2(config-router)# network 2.2.2.2/32 area 0.0.0.1	Advertise network 1.1.1.1/32 in OSPF area 1.
R2(config-router)#network 10.1.1.0/24 area 0.0.0.1	Advertise network 10.1.1.0/24 in OSPF area 1.
R2(config-router)# network 20.1.1.0/24 area 0.0.0.1	Advertise network 20.1.1.0/24 in OSPF area 1.
R3(config-router)#exit	Exit from Router OSPF mode
R2(config)#router bgp 100	Enter Router mode for BGP
R2(config-router)# neighbor 10.1.1.1 remote-as 100	Add neighbor 10.1.1.1 to remote-as 100.
R2(config-router)#neighbor 10.1.1.1 fall-over bfd	Enable BFD option for neighbor
R2(config-router)# neighbor 20.1.1.2 remote-as 100	Add neighbor 20.1.1.2 to remote-as 100.
R2(config-router)# neighbor 20.1.1.2 fall-over bfd	Enable BFD option for neighbor
R2(config-router)#end	Exit from Router BGP mode

R3

R3#configure terminal	Enter configure mode
R3(config)#interface eth2	Enter the Interface configuration mode for eth2.
R3(config-if)#ip address 20.1.1.2/24	Assign IP Address.
R3(config-if)#exit	Exit the Interface configuration mode.
R3(config)# interface lo	Enter interface mode
R3(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address on loopback interface.
R1(config-if)#bfd session 3.3.3.3 1.1.1.1 multihop	Enable BFD multihop session
R2(config-if)#exit	Exit the Interface configuration mode
R3(config)#router ospf 100	Enter Router mode for OSPF
R3(config-router)#ospf router-id 3.3.3.3	Configure router-id in OSPF
R3(config-router)# network 3.3.3.3/32 area 0.0.0.1	Advertise network 3.3.3.3/32 in OSPF area 1.
R3(config-router)# network 20.1.1.0/24 area 0.0.0.1	Advertise network 20.1.1.0/24 in OSPF area 1.
R3(config-router)#exit	Exit from Router OSPF mode
R3(config)#router bgp 100	Enter Router mode for BGP

R3(config-router)# neighbor 1.1.1.1 remote-as 100	Add neighbor 1.1.1.1 to remote-as 100.
R3(config-router)# neighbor 1.1.1.1 fall-over bfd multihop	Enable BFD option for neighbor
R3(config-router)#neighbor 1.1.1.1 update-source lo	Add neighbor 1.1.1.1 to update-source lo.
R3(config-router)# neighbor 20.1.1.1 remote-as 100	Add neighbor 20.1.1.1 to remote-as 100.
R3(config-router)#neighbor 20.1.1.1 fall-over bfd	Enable BFD option for neighbor
R3(config-router)#end	Exit from Router BGP mode

Validation

R1

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1   Full/Backup      00:00:35    10.1.1.2            eth1         0
R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface  Down-
Reason  Remote-Addr
1                    1             IPv4        Single-Hop     Up         00:02:55
eth1      NA                  10.1.1.2/32
257                  0             IPv4        Multi-Hop      Up          00:00:18
NA         NA                    3.3.3.3/32
Number of Sessions:    2


R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10023          Interface name :eth1
Session Index : 1
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                  Session State : Up
Local Discriminator : 1                       Local Address : 10.1.1.1/32
Remote Discriminator : 1                   Remote Address : 10.1.1.2/32
Local Port : 49152                              Remote Port : 3784
```

```
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000814                Pkt Out : 00000000000000000814
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:59

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                   Session Index : 257
Lower Layer : IPv4                                Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                     Local Address : 1.1.1.1/32
Remote Discriminator : 0                     Remote Address : 3.3.3.3/32
Local Port : 49153                                 Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 0                       Neg Rx: 0                       Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                Pkt Out : 00000000000000000107
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
```



```
UP Count : 0                                                    UPTIME : 00:00:00
```

R2

```
R2#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface  Instance ID
1.1.1.1           1   Full/DR         00:00:32      10.1.1.1          eth1         0
3.3.3.3           1   Full/Backup     00:00:40     20.1.1.2           eth2         0


R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1               1               IPv4            Single-Hop    Up         00:02:33
eth1            NA              10.1.1.1/32
2               1               IPv4            Single-Hop    Up         00:01:54
eth2            NA              20.1.1.2/32
Number of Sessions:    2


R2#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10023         Interface name :eth1
Session Index : 1
Lower Layer : IPv4                           Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                    Local Address : 10.1.1.2/32
Remote Discriminator : 1                Remote Address : 10.1.1.1/32
Local Port : 49152                           Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                  Min Rx: 250                  Multiplier: 3
Neg Tx: 250                  Neg Rx: 250                  Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
```

```
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000713                Pkt Out : 00000000000000000714
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:37

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 10053          Interface name :eth2
Session Index : 2
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                     Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32
Local Port : 49153                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                    Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000535              Pkt Out : 00000000000000000537
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:58

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

R3

```
R3#show ip ospf neighbor

Total number of full neighbors: 1
```

```
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1     Full/DR         00:00:36    20.1.1.1          eth1            0


R3#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1                    2          IPv4            Single-Hop      Up         00:01:21
eth1            NA                20.1.1.1/32
257                  1          IPv4            Multi-Hop       Up        00:00:00
NA              NA                1.1.1.1/32
Number of Sessions:    2
Total number of Established sessions 2


R3#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10053          Interface name :eth1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 20.1.1.2/32
Remote Discriminator : 2                 Remote Address : 20.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000391                Pkt Out : 00000000000000000391
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
```

```
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:01:26

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                  Session Index : 257
Lower Layer : IPv4                                Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                   Local Address : 3.3.3.3/32
Remote Discriminator : 1                    Remote Address : 1.1.1.1/32
Local Port : 49153                                Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                         Min Rx: 250                    Multiplier: 3
Neg Tx: 250                         Neg Rx: 250                    Neg detect mult:250
Min echo Tx: 1000              Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000               Pkt Out : 00000000000000000047
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

CHAPTER 3 BFD Static Route Configuration

This chapter describes the configurations for BFD static routes.

In order to establish alternate paths to destinations that have the least possible delay it is important to quickly detect any changes to static route validity. BFD detects the liveliness of a static route's nexthop and then uses the nexthop's reachability information to determine whether routes are valid. Using BFD to reach a static route's nexthop also ensures that a static route is inserted in the forwarding database only when the nexthop neighbor is reachable.

Topology

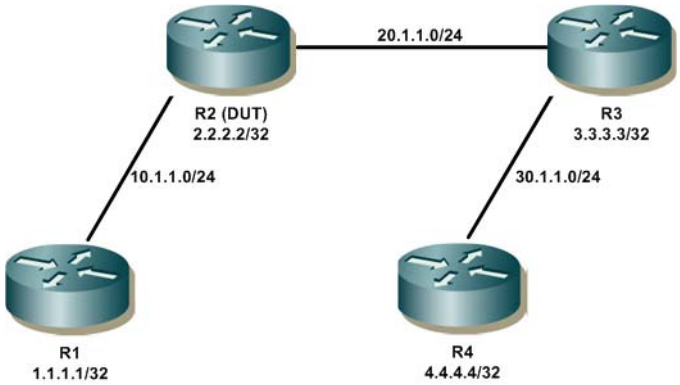


Figure 3-110: BFD Static Route Basic Topology

R1

`R1(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address on interface.
`R1(config-if)#exit`	Exit the Interface configuration mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#ip route 30.1.1.0/24 20.1.1.3`	Configure static route.
`R2(config)#ip bfd static all-interfaces`	Enable BFD for all static routes.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip static bfd`	Enable static BFD on the interface.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#ip static 30.1.1.0/24 20.1.1.3 fall-over bfd`	Enable static BFD at static route level.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.

R3

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#ip route 10.1.1.0/24 20.1.1.2`	Configure static route.
`R3(config)#ip bfd static all-interfaces`	Enable BFD for all static routes.
`R3(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R3(config-if)#ip address 20.1.1.3/24`	Assign IP address on interface.
`R3(config-if)#ip static bfd`	Enable static BFD at interface level.
`R3(config-if)#exit`	Exit the Interface configuration mode.
`R3(config)#ip static 10.1.1.0/24 20.1.1.2 fall-over bfd`	Enable static BFD at static route level.
`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 30.1.1.2/24`	Assign IP address on interface.
`R3(config-if)#exit`	Exit the Interface configuration mode.

R4

`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 30.1.1.1/24`	Assign IP address on interface.
`R3(config-if)#exit`	Exit the Interface configuration mode.

Validation

R2

```
#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-
Addr
5          1            IPv4         Single-Hop  Up          00:09:32
20.1.1.3/32
Number of Sessions:    1
VPC2#sh bfd session detail
=====================================================

Session Interface Index : 3             Session Index : 5
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 5                 Local Address : 20.1.1.2/32
Remote Discriminator : 1                Remote Address : 20.1.1.3/32
Local Port : 49156                      Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
```

```
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000a29                Pkt Out : 0000000000000bb6
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:09:34

Protocol Client Info:
RIB-> Client ID: 42      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R3

```
#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-
Addr
1          5            IPv4         Single-Hop  Up          00:09:39
20.1.1.2/32
Number of Sessions:    1
VPC3#sh bfd session detail
============================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 20.1.1.3/32
Remote Discriminator : 5                 Remote Address : 20.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000a59                Pkt Out : 0000000000000a53
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:09:41

Protocol Client Info:
RIB-> Client ID: 42      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

CHAPTER 4 BFD Authentication

This chapter provides BFD authentication configuration examples.

Overview

Bidirectional Forwarding Detection (BFD) is a protocol intended to detect faults in the bidirectional path between two forwarding engines, including physical interfaces, sub-interfaces, and data link. It operates independently of media, data protocols, and routing protocols. A session will be created between links. When BFD links is hacked, the link may be falsely declared to be down, or falsely declared to be up. To overcome this type of situations, need to use authentication on BFD. Using this we can mitigate threats from attackers.

OcNOS supports the following authentication types:

- Simple password
- Meticulous-Keyed-SHA1
- Keyed-SHA1

Among these types, Meticulous-Keyed-SHA1 is the strongest one.

Authentication is optionally enabled on BFD sessions. By default, it is disabled and is configurable via CLI. When authentication is enabled, BFD packets will exchange with authentication section (based on the configured auth type). Receiving system will examine the authentication section of the packet; if it is successful then it will accept. Otherwise, it will discard.

Enabling BFD Authentication for Multihop for IPv4, Using Key-ID

In this example, the BFD Multihop session is configured between R1 and R3 using single key (using key-ID). Once the BFD session is up, the authentication is enabled on both the routers, with the authentication type as Keyed-SHA1. We can enable the authentication on BFD session using any one of the above mentioned authentication type, with the Identical authentication type on both side.

Note: BFD authentication is not supported for Single hop BFD session.

Topology

Figure 4-111: Basic Topology of Three Routers

Router 1 (R1)

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface lo`	Enter the Loopback Interface configuration mode.
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.

`R1(config)#interface xe9`	Enter Interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 20.1.1.2 multihop`	Enabling BFD Multihop session
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#redistribute connected`	
`R1(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 20.1.1.2 auth type keyed-sha1 key-id 2 key ocnos`	Enabling Authentication for Multihop session

Router 2 (R2)

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface lo`	Enter the Loopback Interface configuration mode.
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#interface xe9`	Enter Interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#interface xe2`	Enter Interface Mode.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#router ospf 1`	Enter router OSPF mode
`R2(config-router)#redistribute connected`	
`R2(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#exit`	Exit router OSPF mode

Router 3 (R3)

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#interface lo`	Enter the Loopback Interface configuration mode.
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Assign IP address for interface
`R3(config-if)#exit`	Exit from interface mode.
`R3(config)#interface xe2`	Enter Interface Mode.
`R3(config-if)#ip address 20.1.1.2/24`	Assign IP address for interface
`R3(config-if)#bfd session 20.1.1.2 10.1.1.1 multihop`	Enabling BFD Multihop session

R3(config-if)#exit	Exit from interface mode.
R3(config)#router ospf 1	Enter router OSPF mode
R3(config-router)#redistribute connected	
R3(config-router)#network 20.1.1.0/24 area 0	Advertise the network to area 0
R3(config-router)#exit	Exit router OSPF mode
R3(config)#bfd multihop-peer 10.1.1.1 auth type keyed-sha1 key-id 2 key ocnos	Enabling Authentication for Multihop session

Validation

Check Multihop session is up between R1 and R3 with authentication type configured.

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:33    10.1.1.2        xe9
0

R1#sh bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface       Down-Reason  Remote-Addr
1001       1001         IPv4         Multi-Hop   Up          00:34:32  NA
NA            20.1.1.2/32
Number of Sessions:    1

R1#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
======

Session Interface Index : 0              Session Index : 1001
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 1001               Local Address : 10.1.1.1/32
Remote Discriminator : 1001              Remote Address : 20.1.1.2/32
Local Port : 49152                       Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
```

```
    Bfd GTSM Disabled
    Bfd Authentication Enabled
    Authentication type : keyed-sha1
    Authentication Key-id : 2

    Counters values:
    Pkt In : 00000000000000027907                Pkt Out : 00000000000000028347
    Pkts Drop : 0000000000000000000              Auth Pkts Drop :
    00000000000000000000
    Echo Out : 0000000000000000000               IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 0000000000000000000            IPv6 Pkt Out : 0000000000000000000
    UP Count : 12                                UPTIME : 00:34:34

    Protocol Client Info:
    BFD-> Client ID: 28  Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    1

    R3#show ip ospf neighbor

    Total number of full neighbors: 1
    OSPF process 1 VRF(default):
    Neighbor ID    Pri   State           Dead Time   Address         Interface
    Instance ID
    2.2.2.2         1   Full/Backup     00:00:32   20.1.1.1       xe2
    0

    R3#sh bfd session

    BFD process for VRF: (DEFAULT VRF)
    ================================================================================
    =======
    Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
    Interface      Down-Reason  Remote-Addr
    1001      1001        IPv4        Multi-Hop   Up         00:36:27  NA
    NA           10.1.1.1/32
    Number of Sessions:    1

    R3#sh bfd session detail

    BFD process for VRF: (DEFAULT VRF)
    ================================================================================
    ======

    Session Interface Index : 0              Session Index : 1001
    Lower Layer : IPv4                       Version : 1
    Session Type : Multihop Arbit Path       Session State : Up
    Local Discriminator : 1001               Local Address : 20.1.1.2/32
    Remote Discriminator : 1001              Remote Address : 10.1.1.1/32
    Local Port : 49152                       Remote Port : 4784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250               Min Rx: 250               Multiplier: 3
    Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
```

```
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Enabled
Authentication type : keyed-sha1
Authentication Key-id : 2

Counters values:
Pkt In : 00000000000000028428                Pkt Out : 00000000000000028715
Pkts Drop : 00000000000000000000             Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000              IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 12                                UPTIME : 00:36:29

Protocol Client Info:
BFD-> Client ID: 28  Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

CHAPTER 5 BFD with VRF Configuration

This chapter shows using BFD with user defined VRF for OSPFv2 and OSPFv3.

Topology

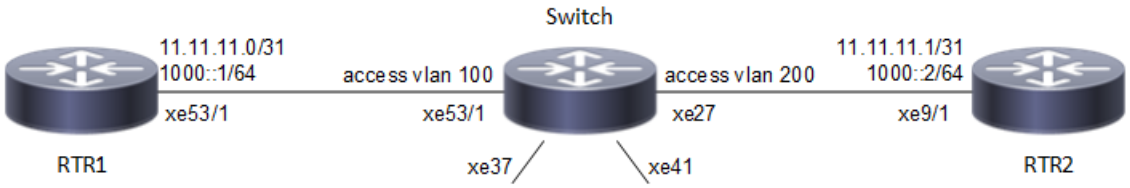


Figure 5-112: BFD user-defined VRF

RTR1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf10`	Create VRF instance with VRF10 and enter into VRF mode
`(config-vrf)#exit`	Exit from VRF mode
`(config)#interface xe53/1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf10`	Enable VRF forwarding on interface
`(config-if)#ip address 11.11.11.0/31`	Assign IPv4 address in /31 mask.
`(config-if)#ipv6 address 1000::1/64`	Assign IPv6 address in /64 mask.
`(config-if)#ipv6 router ospf area 0 tag vrf10`	Tag OSPFv3 instance on interface with VRF10 for area 0
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 65535 vrf10`	Enter into OSPF VRF configuration mode
`(config-router)#router-id 1.1.1.1`	Assign router ID 1.1.1.1 for OSPF process 65535
`(config-router)#bfd all-interfaces`	Enable BFD for all-interface into OSPF
`(config-router)#network 11.11.11.0/31 area 0`	Enable routing for network 11.11.11.0/31 in area 0
`(config-router)#exit`	Exit from OSPF VRF configuration mode
`(config)#router ipv6 vrf ospf vrf10`	Enter into IPv6 OSPF VRF configuration mode
`(config-router)#router-id 2.2.2.2`	Assign router-id 2.2.2.2 for IPv6 OSPF process
`(config-router)#bfd all-interfaces`	Enable BFD for all-interface into OSPF
`(config-router)#exit`	Exit from IPv6 OSPF VRF configuration mode

Switch

`#configure terminal`	Enter configure mode.
`(config)#bridge 32 protocol rstp vlan-bridge`	Create a RSTP VLAN aware bridge with bridge-id 32
`(config)#vlan 100 bridge 32`	Create VLAN 100 and map it to bridge 32
`(config)#vlan 200 bridge 32`	Create VLAN 200 and map it to bridge 32
`(config)#interface xe53/1`	Enter interface mode

(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 100	Map the VLAN 100 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe27	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 200	Map the VLAN 200 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe37	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 100	Map the vlan 100 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe41	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)# bridge-group 32 spanning-tree disable	Configure bridge group to l2 interface with spanning-tree disable
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 200	Map the VLAN 200 to access interface
(config-if)#exit	Exit interface mode.

RTR2

#configure terminal	Enter configure mode.
(config)#ip vrf vrf10	Create VRF instance with VRF10 and enter into vrf mode
(config-vrf)#exit	Exit from VRF mode
(config)#interface xe9/1	Enter interface mode
(config-if)#ip vrf forwarding vrf10	Enable VRF forwarding on interface
(config-if)#ip address 11.11.11.1/31	Assign IPv4 address in /31 mask.
(config-if)#ipv6 address 1000::2/64	Assign IPv6 address in /64 mask.
(config-if)#ipv6 router ospf area 0 tag vrf10	Tag OSPFv3 instance on interface with VRF10 for area 0
(config-if)#exit	Exit interface mode.
(config)#router ospf 65535 vrf10	Enter into OSPF VRF configuration mode
(config-router)#router-id 3.3.3.3	Assign router ID 3.3.3.3 for OSPF process 65535
(config-router)#bfd all-interfaces	Enable BFD for all-interface into OSPF
(config-router)#network 11.11.11.0/31 area 0	Enable routing for network 11.11.11.0/31 in area 0
(config-router)#exit	Exit from OSPF VRF configuration mode

(config)#router ipv6 vrf ospf vrf10	Enter into IPv6 OSPF VRF configuration mode
(config-router)#router-id 4.4.4.4	Assign router-id 4.4.4.4 for IPv6 OSPF process
(config-router)#bfd all-interfaces	Enable BFD for all-interface into OSPF
(config-router)#exit	Exit from IPv6 OSPF VRF configuration mode

Validation

RTR1

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 65535 VRF(vrf10):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
3.3.3.3           1   Full/Backup     00:00:32    11.11.11.1      xe15
0

#sh bfd session vrf vrf10

BFD process for VRF: vrf10
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface       Down-Reason  Remote-Addr
256       256          IPv6        Single-Hop  Up          00:26:26  xe15
NA            fe80::eac5:7aff:fe64:4a1d/128
1         1            IPv4        Single-Hop  Up          00:19:05  xe15
NA            11.11.11.1/32
Number of Sessions:    2

#sh bfd session vrf vrf10 detail

BFD process for VRF: vrf10
================================================================================
======

Session Interface Index : 10016          Interface name :xe15
Session Index : 256
Lower Layer : IPv6                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 256                Local Address :
fe80::eac5:7aff:fe78:711d/128
Remote Discriminator : 256               Remote Address :
fe80::eac5:7aff:fe64:4a1d/128
Local Port : 49153                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
```

```
    Sess Down Reason : NA
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : n/a                                Pkt Out : n/a
    Pkts Drop : 00000000000000000000            Auth Pkts Drop :
    00000000000000000000
    Echo Out : 00000000000000000000             IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 00000000000000007256          IPv6 Pkt Out : 00000000000000007256
    UP Count : 1                                UPTIME : 00:26:28

    Protocol Client Info:
    OSPF6-> Client ID: 5  Flags: 4
    ------------------------------------------------------------

    Session Interface Index : 10016          Interface name :xe15
    Session Index : 1
    Lower Layer : IPv4                       Version : 1
    Session Type : Single Hop                Session State : Up
    Local Discriminator : 1                  Local Address : 11.11.11.0/32
    Remote Discriminator : 1                 Remote Address : 11.11.11.1/32
    Local Port : 49154                       Remote Port : 3784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250               Min Rx: 250               Multiplier: 3
    Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Sess Down Reason : NA
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : n/a                                Pkt Out : n/a
    Pkts Drop : 00000000000000000000            Auth Pkts Drop :
    00000000000000000000
    Echo Out : 00000000000000000000             IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
    UP Count : 1                                UPTIME : 00:19:07

    Protocol Client Info:
    OSPF-> Client ID: 4  Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    2
```

RTR3

```
    #sh ip ospf neighbor

    Total number of full neighbors: 1
    OSPF process 65535 VRF(vrf10):
```

```
Neighbor ID    Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1         1   Full/DR         00:00:31    11.11.11.0      xe10
0

#sh ipv6 ospf neighbor

Total number of full neighbors: 1
OSPFv3 Process (vrf10)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:28    xe10       0

#sh bfd session vrf vrf10

BFD process for VRF: vrf10
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1         1           IPv4        Single-Hop  Up         00:20:44  xe10
NA           11.11.11.0/32
256       256         IPv6        Single-Hop  Up         00:28:05  xe10
NA           fe80::eac5:7aff:fe78:711d/128
Number of Sessions:    2

#sh bfd session vrf vrf10 detail

BFD process for VRF: vrf10
================================================================================
======

Session Interface Index : 10011          Interface name :xe10
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 11.11.11.1/32
Remote Discriminator : 1                 Remote Address : 11.11.11.0/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                                Pkt Out : n/a
Pkts Drop : 00000000000000000000            Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000             IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
```

```
    UP Count : 2                                UPTIME : 00:20:46

    Protocol Client Info:
    OSPF-> Client ID: 4  Flags: 4
    ------------------------------------------------------------

    Session Interface Index : 10011          Interface name :xe10
    Session Index : 256
    Lower Layer : IPv6                       Version : 1
    Session Type : Single Hop                Session State : Up
    Local Discriminator : 256                Local Address :
    fe80::eac5:7aff:fe64:4a1d/128
    Remote Discriminator : 256               Remote Address :
    fe80::eac5:7aff:fe78:711d/128
    Local Port : 49153                       Remote Port : 3784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250               Min Rx: 250               Multiplier: 3
    Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Sess Down Reason : NA
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : n/a                               Pkt Out : n/a
    Pkts Drop : 00000000000000000000           Auth Pkts Drop :
    00000000000000000000
    Echo Out : 00000000000000000000            IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 00000000000000007707         IPv6 Pkt Out : 00000000000000007718
    UP Count : 1                               UPTIME : 00:28:07

    Protocol Client Info:
    OSPF6-> Client ID: 5  Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    2
```

BFD Over Static Routing IPv4 and IPv6

RTR1

#configure terminal	Enter configure mode.
(config)#ip vrf vrf10	Create VRF instance with VRF10 and enter into VRF mode
(config-vrf)#exit	Exit from VRF mode
(config)#ip bfd vrf vrf10 static all-interfaces	Enable global IPv4 BFD config for user defined VRF interfaces
(config)#ipv6 bfd vrf vrf10 static all-interfaces	Enable global IPv6 BFD config for user defined VRF interfaces
(config)#interface xe53/1	Enter interface mode
(config-if)#ip vrf forwarding vrf10	Enable VRF forwarding on interface
(config-if)#ip address 11.11.11.0/31	Assign IPv4 address in /31 mask.
(config-if)#ipv6 address 1000::1/64	Assign IPv6 address in /64 mask.
(config-if)#exit	Exit interface mode.
(config)#ip route vrf vrf10 200.200.200.200/32 11.11.11.1 xe53/1	Create IPv4 VRF static route for static BFD session
(config)#ipv6 route vrf vrf10 2000::/64 1000::2 xe53/1	Create IPv6 VRF static route for static BFD session
(config)#exit	Exit from configuration mode

RTR2

#configure terminal	Enter configure mode.
(config)#ip vrf vrf10	Create VRF instance with VRF10 and enter into VRF mode
(config-vrf)#exit	Exit from VRF mode
(config)#ip bfd vrf vrf10 static all-interfaces	Enable global IPv4 BFD config for user defined VRF interfaces
(config)#ipv6 bfd vrf vrf10 static all-interfaces	Enable global IPv6 BFD config for user defined VRF interfaces
(config)#interface xe9/1	Enter interface mode for xe9/1
(config-if)#ip vrf forwarding vrf10	Enable VRF forwarding on interface
(config-if)#ip address 11.11.11.1/31	Assign IPv4 address in /31 mask.
(config-if)#ipv6 address 1000::2/64	Assign IPv6 address in /64 mask.
(config-if)#exit	Exit interface mode.
(config)# ip route vrf vrf10 100.100.100.100/32 11.11.11.0 xe9/1	Create IPv4 VRF static route for static BFD session
(config)# ipv6 route vrf vrf10 3000::2/64 1000::1 xe9/1	Create IPv6 VRF static route for static BFD session
(config)#exit	Exit from configuration mode

Validation

RTR1

```
#show bfd session vrf vrf10
 BFD process for VRF: vrf10
================================================================================
=============
Sess-Idx  Remote-Disc  Lower-Layer  Sess-Type  Sess-State  UP-Time  Inter-
face  Down-Reason  Remote-Addr
3                  4            IPv4              Single-Hop      Up
00:14:13    xe53/ 1        NA          11.11.11.1/32
4                  5            IPv6              Single-Hop      Up
00:13:24    xe53/ 1        NA           1000::2/128
Number of Sessions:    2


R1#show bfd session vrf vrf10 detail
BFD process for VRF: vrf10
================================================================================
==========

Session Interface Index : 4              Interface name :xe53/1
Session Index : 1
Lower Layer : IPv4                             Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                      Local Address : 11.11.11.0/32
Remote Discriminator : 1                 Remote Address : 11.11.11.1/32
Local Port : 49152                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                     Neg detect
mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000001184                  Pkt Out :
00000000000000001184
Echo Out : 00000000000000000000            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out :
00000000000000000000
UP Count : 1                                                    UPTIME :
00:00:21

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
```

```
Session Interface Index : 4              Interface name :xe53/1
Session Index : 2
Lower Layer : IPv6                             Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                      Local Address :
fe80::5054:ff:fed0:e0c1/128
Remote Discriminator : 2                 Remote Address :
fe80::5054:ff:fe3d:af2b/128
Local Port : 49153                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                      Min Rx: 250                    Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                      Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                  Pkt Out :
00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000001158         IPv6 Pkt Out :
00000000000000001163
UP Count : 1                                   UPTIME : 00:00:14

Protocol Client Info:
OSPF6-> Client ID: 5     Flags: 4
------------------------------------------------------------
Number of Sessions:    2


R1#show bfd
BFD ID: 00      Start Time:Tue Mar 19 13:31:08 2019
 BFD Admin State: UP
Number of Sessions:    2
Slow Timer: 2000                      Image type: MONOLITHIC
Echo Mode: Disabled                BFD Notifications disabled
Next Session Discriminator:    3
```

RTR2

```
#show bfd session vrf vrf10
BFD process for VRF: vrf10
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface  Down-Reason  Remote-Addr
```

```
4                  3                              IPv4              Single-Hop
Up       00:15:39     xe9/1       NA              11.11.11.0/32
5                  4                              IPv6              Single-Hop
Up           00:14:50      xe9/1           NA                 1000::1/128
Number of Sessions:    2



R2#show bfd session vrf vrf10 detail
BFD process for VRF: vrf10
================================================================================
=======
Session Interface Index : 3               Interface name :xe9/1
Session Index : 1
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 1                      Local Address : 11.11.11.1/32
Remote Discriminator : 1                 Remote Address : 11.11.11.0/32
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                     Min Rx: 250                     Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                     Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000001661                   Pkt Out : 00000000000000001665
Echo Out : 00000000000000000000           IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                    UPTIME :
00:00:53

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------

Session Interface Index : 3             Interface name :xe9/1
Session Index : 2
Lower Layer : IPv6                            Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 2                     Local Address :
fe80::5054:ff:fe3d:af2b/128
Remote Discriminator : 2                Remote Address :
fe80::5054:ff:fed0:e0c1/128
Local Port : 49153                              Remote Port : 3784
Options :

Diagnostics : None
```



```
Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                    Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                 Pkt Out : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000001642        IPv6 Pkt Out : 00000000000000001636
UP Count : 1                                                  UPTIME :
00:00:56

Protocol Client Info:
OSPF6-> Client ID: 5     Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

Bidirectional Forwarding Detection Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Bidirectional Forwarding Commands

This chapter explains the commands used to configure Bidirectional Forwarding (BFD):

bfd auth type

Use this command to enable BFD authentication on an interface that has either an IPv4 or an IPv6 BFD session.

Use the no form of the command to disable BFD authentication.

Note: BFD authentication is not supported for single hop IPv4 sessions.

Command Syntax

```
bfd auth type (simple | keyed-sha1 | meticulous-keyed-sha1) (key-id <0-255> key
  LINE)
no bfd auth
```

Parameters

`simple`	Specify a simple authentication type.
`keyed-sha1`	Specify a keyed secure hashing algorithm authentication type.
`meticulous-keyed-sha1`	Specify an authentication key meticulous keyed secure hashing algorithm authentication.
`key-id`	Indicate the `key-id` keyword.
`<0-255>`	Specify the key ID value.
`key`	Indicate the `key` keyword.
`LINE`	Specify the authentication key name.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Do the following to configure a single-key support:

```
(config)#interface eth1
(config-if)#bfd auth type simple key-id 14 key myid1
```

bfd

Use this command to enable and disable all the BFD sessions on this interface.

Command Syntax

```
bfd (enable|disable)
```

Parameters

`enable`	Enable BFD
`disable`	Disable BFD

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd disable
```

bfd echo

Use this command to set BFD sessions to echo mode.

Use the no form of the command to return a BFD session to its default mode.

Note: BFD echo mode is supported for IPv4 BFD single hop sessions only.

Command Syntax

```
bfd echo
no bfd echo
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd echo
```

bfd echo interval

Use this command to set the BFD echo interval.

Use the no form of this command to reset the echo interval to its default value.

Command Syntax

```
bfd echo interval <50-4294967>
no bfd echo interval <50-4294967>
```

Parameter

<50-4294967>	Transmit interval in milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command sets the BFD echo with no values.

```
#configure terminal
(config)#interface eth1
(config-if)#bfd echo interval 234
```

bfd-firmware

Use this command to enable multi-hop or micro-BFD processing in hardware.

Note: For LAG interfaces, you must specify `micro-bfd`. With `micro-bfd` only single hop sessions are supported.

Command Syntax

```
bfd-firmware (multi-hop|micro-bfd)
```

Parameter

`multi-hop`	Enable multihop sessions
`micro-bfd`	Enable micro-BFD sessions (default)

Default

By default, micro-BFD sessions are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd-firmware multi-hop
```

bfd interval

Use this command to configure BFD transmit and receive intervals, and the hello multiplier value.

Use the no form of the command to set the intervals and multiplier to their default values.

Command Syntax

```
bfd interval <3-999> minrx <3-999> multiplier <3-50>
no bfd interval <3-999> minrx <3-999> multiplier <3-50>
```

Parameters

<3-999>	Transmit interval in milliseconds.
minrx	Receive interval.
<3-999>	Receive interval in milliseconds.
multiplier	Hello multiplier.
<3-50>	Hello multiplier value.

Defaults

The default for the transmit and receive intervals is 250 milliseconds.

The default hello multiplier value is 3.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd interval 100 minrx 100 multiplier 5
(config-if)#
```

bfd multihop-peer

Use this command to enable authentication over either a multihop IPv4 or IPv6 session

Use the no form of the command to disable BFD authentication.

Command Syntax

```
bfd multihop-peer (A.B.C.D|X:X::X:X) auth type (simple | keyed-sha1 | meticulous-
  keyed-sha1) key-id <0-255> key LINE
no bfd multihop-peer (A.B.C.D) auth
```

Parameters

`A.B.C.D`	Specify an IPv4 address.
`auth type`	Specify an authentication type.
`simple`	Specify a simple authentication type.
`keyed-sha1`	Specify a keyed secure hashing algorithm authentication type.
`meticulous-keyed-sha1`	Specify an authentication key Meticulous Keyed Secure hashing algorithm authentication type.
`key-id`	Indicate the `key-id` keyword.
`<0-255>`	Specify the key ID value.
`key`	Indicate the `key` keyword.
`LINE`	Specify the authentication key name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Do the following to configure a single-key support:

```
#configure terminal
(config)#bfd multihop-peer 123.12.1.2 auth-type simple key-id 14 key myid1
```

bfd multihop-peer A.B.C.D interval

Use this command to configure IPv4 BFD multihop peer timer values.

Use the no form of the command to reset the IPv4 multihop peer timer value.

Command Syntax

```
bfd multihop-peer A.B.C.D interval <50-999> minrx <50-999> multiplier <3-50>
no bfd multihop-peer A.B.C.D interval <50-999> minrx <50-999> multiplier <3-50>
```

Parameters

`interval`	Indicate the interval parameter.
`<50-999>`	Specify the actual transmit interval in milliseconds.
`minrx`	Indicate the minrx parameter.
`<50-999>`	Specify the actual reception interval in milliseconds.
`multiplier`	Indicate the multiplier parameter.
`<3-50>`	Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Multiplier value is 3

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd multihop-peer 10.1.1.67 interval 100 minrx 100 multiplier 3
(config)#
```

bfd multihop-peer X:X::X:X interval

Use this command to configure an IPv6 BFD multihop peer timer values.

Use the no form of the command to reset the IPv6 multihop peer timer values.

Command Syntax

```
bfd multihop-peer X:X::X:X interval <50-999> minrx <50-999> multiplier <3-50>
no bfd multihop-peer X:X::X:X interval <50-999> minrx <50-999> multiplier <3-50>
```

Parameters

`interval`	Indicate the interval parameter.
`<50-999>`	Specify the actual transmit interval in milliseconds.
`minrx`	Indicate the minrx parameter.
`<50-999>`	Specify the actual reception interval in milliseconds.
`multiplier`	Indicate the multiplier parameter.
`<3-50>`	Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Default multiplier value is 3

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd multihop-peer 10.1.1.1 interval 100 minrx 100 multiplier 3
```

bfd notification

Use this command to enable or disable BFD notification.

Command Syntax

```
bfd notification (enable | disable)
```

Parameters

`disable`	Disable BFD notification.
`enable`	Enable BFD notification.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bfd notification enable

(config)#bfd notification disable
```

bfd slow-timer

Use this command to set a BFD slow timer interval.

Use the no form of the command to reset the timer to default values.

Command Syntax

```
bfd slow-timer <1000-30000>
no bfd slow-timer
```

Parameter

<1000-30000>	Interval for the slow-timer in milliseconds

Command Mode

Configure mode

Default

Default slow-timer value is 2000

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd slow-timer 1500
(config)#
```

debug bfd

Use this command to enable debugging for BFD.

Use the no form of the command to disable all debugging for BFD.

Command Syntax

```
debug bfd (all|)
debug bfd (event|ipc-error|ipc-event|nsm|packet|session)
no debug bfd (all|)
no debug all
no debug all bfd
no debug bfd (event|ipc-error|ipc-event|nsm|packet|session)
```

Parameters

`all`	Enable all debugging.
`event`	Enable BFD event debugging.
`ipc-error`	Enable BFD IPC-error debugging
`ipc-event`	Enable BFD IPC-event debugging.
`nsm`	Enable BFD NSM debugging.
`packet`	Enable BFD packet debugging.
`session`	Enable BFD session debugging.

Command Mode

Exec, Privileged Exec and Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug bfd all
#no debug bfd all
#debug bfd event
#debug bfd ipc-error
#debug bfd ipc-event
#debug bfd nsm
#debug bfd packet
#debug bfd session
```

hardware-profile micro-bfd

Use this command to enable micro-BFD support on hardware.

Note: Micro-bfd support is optional when a BFD session is configured over a LAG interface between two Qumran devices. It is mandatory to enable micro-bfd when the BFD session is configured over LAG interface between different platforms. When BFD sessions are configured over LAG interfaces, both Qumran nodes should have micro-bfd enabled or disabled.

Command Syntax

```
hardware-profile micro-bfd (enable|disable)
```

Parameter

`enable`	Enable micro-bfd support on Qumran
`disable`	Disable micro-bfd support on Qumran

Default

By default, micro-bfd support is disabled on Qumran.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)# hardware-profile micro-bfd enable
```

key

Use this command to manage, add or delete authentication keys in a key chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax

```
key <0-2147483647>
no key <0-2147483647>
```

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, BFD uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```

key chain

Use this command to enter key chain mode to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax

```
key chain WORD
no key chain WORD
```

Parameters

WORD	Specify the name of the key chain to manage.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035>
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite
send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646>
send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646>
no send-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.
`MONTH`	Specify the month of the year to start as the first three letters of the month, for example, Jan.
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to end.
`MONTH`	Specify the month of the year to end as the first three letters of the month, for example, Jan.
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
```

```
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#send-lifetime 03:03:01 Jan 3 2004 04:04:02 Dec 6 2006
```

show bfd

Use this command to display information about the BFD process.

Command Syntax

```
show bfd
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd
BFD ID: 00      Start Time:Fri May 1 09:55:06 2009
Number of Sessions:     1
Slow Timer: 1000        Image type: MONOLITHIC
Echo Mode: Disabled     Next Session Discriminator:    2
#
```

Table 1-67 explains the output fields.

Table 1-67: show BFD fields

Entry	Description
BFD ID	ID number of the BFD session.
Start Time	The date and time when the BFD session was started
BFD Admin State	State of the BFD session: Initializing: session is initializing Up: session is up. Down: session is down
Number of Sessions	Number of BFD sessions running on the device.
Slow Timer	Required minimum transmission time for the BFD session.
Image Type	Distributed or Monolithic.
Echo Mode	Either enabled or disabled.
Next Session Discriminator	An opaque discriminator value that identifies each session on the device that is used to demultiplex multiple BFD sessions between the same pair of devices.

show bfd interface

Use this command to display details for an interface running BFD or for all interfaces configured for BFD.

Command Syntax

```
show bfd interface (ifindex <0-4294967295>|all|)
```

Parameters

`all`	Display all interfaces.
`ifindex`	Display an interface index.
`<0-4294967295>`	Display an ID of an interface in this range.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd interface all
Interface:         lo ifindex: 1 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth0 ifindex: 2 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth1 ifindex: 3 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       sit0 ifindex: 4 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       gre0 ifindex: 5 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5
```

Table 1-68 explains the output fields.

Table 1-68: show BFD interface fields

Entry	Description
interface	Interface on which BFD is running
ifindex	Interface index number
state	State of the BFD session for the interface: UP: session is up. DOWN: session is down
Interface level configuration	State of interface-level properties: echo on or off slow-timer (timer dampening) on or off
Min Tx	The minimum interval that the local device would like to use when transmitting BFD control packets.
Min Rx	The minimum interval between received BFD control packets that this device is capable of supporting
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving device in asynchronous mode.

show bfd session

Use this command to display BFD sessions.

Note: BFD Packet In and BFD Packet Out counters are not supported for Single Hop IPv4 BFD sessions on Qumran devices.

Command Syntax

```
show bfd session (detail|)
show bfd session vrf (WORD|all|default) (detail|)
```

Parameters

`detail`	Session details.
`WORD`	Sessions for this user-defined Virtual Routing and Forwarding instance name.
`all`	Show information for all Virtual Routing and Forwarding instances
`default`	Show information for only the default Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bfd session detail
Session Interface Index : 3                Session Index : 1
Lower Layer : IPv4                         Version : 1
Session Type : Single Hop                  Session State : Down
Local Discriminator : 1                    Local Address : 19.19.19.2/32
Remote Discriminator : 0                   Remote Address : 19.19.19.1/32
Local Port : 49152                         Remote Port : 3784
Options :

Diagnostics: None

Timers in Milliseconds :
Min Tx: 20                 Min Rx: 20                 Multiplier: 5
Neg Tx: 0                  Neg Rx: 0                  Neg detect mult: 0
Min echo Tx: 20            Min echo Rx: 10            Neg echo intrvl: 0
Storage type: 2
Sess down time: 00:00:00
Bfd Authentication Enabled
Authentication type : simple
Auth-Key-Id: 47

Counters values:
Pkt In : 0000000000000000                  Pkt Out : 0000000000000011
Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 0                               UPTIME : 00:00:00
```

```
Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------


#show bfd session vrf all

BFD process for VRF: vrf1
========================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          1           IPv4         Single-Hop  Up          00:05:38  eth1
NA           1.1.1.2/32
Number of Sessions:    1

BFD process for VRF: (DEFAULT VRF)
========================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          7           IPv4         Single-Hop  Up          00:03:31  eth3
NA           3.3.3.2/32
2          9           IPv4         Single-Hop  Up          00:00:45  eth4
NA           4.4.4.2/32
Number of Sessions:    2

BFD process for VRF: vrf2
========================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          6           IPv4         Single-Hop  Up          00:03:37  eth2
NA           2.2.2.2/32
Number of Sessions:    1
```

Table 1-69 explains the output fields.

Table 1-69: show bfd session detail fields

Entry	Description
Session Interface Index	ID number of the interface.
Session Index Sess-Idx	ID number of this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried: IPv4 IPv6 MPLS LSP MPLS VCCV MPLS-TP
Version	Session version number; generally 1.

Table 1-69: show bfd session detail fields (Continued)

Entry	Description
Session Type Sess-Type	Single Hop Multihop Arbit Path Multihop OOB Signalled Multihop Unidirectional.
Session State Sess-State	The State of the session: Init: The session is initializing Up: The session is up. Down: The session is down AdminDown: The session has been administratively shutdown indefinitely.
Local Discriminator	A unique discriminator value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Local Address	Local address of the transmitting device.
Remote Discriminator Remote-Disc	The discriminator received from the corresponding remote device; zero if that value is unknown.
Remote Address Remote-Addr	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of destination.
Options	Fate Shared Echo Enabled Demand Enabled Remote Demand Enbl Remote admin Down Poll seq Init.
Diagnostics	Performance diagnostics: None Control Detection Time Expired Echo Failed Neighbor Session Down Forwarding Plane Reset Path Down Concatenated Path Down Admin Down Reverse Concatenated Path Down
Min Tx	Minimum transmit interval.
Min Rx	Minimum receive interval.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
Neg Tx	Negotiated transmit interval.
Neg Rx	Negotiated receive interval in milliseconds.

Table 1-69: show bfd session detail fields (Continued)

Entry	Description
Neg detect mult	Negotiated detection multiplier.
Min echo Tx	Minimum echo transmit interval in milliseconds.
Min echo Rx	Minimum echo receive interval in milliseconds.
Neg echo intrvl	Negotiated echo interval.
Storage type	SNMPv2 storage type (usually be set to 2): other(1) volatile(2) non-Volatile(3) permanent(4 read-Only(5)
Sess down time	Length of time this BFD session has been down.
Bfd GTSM	Whether the BFD session has enabled or disabled the Generalized TTL Security Mechanism (GTSM), which uses the time to live (TTL) or hop count to prevent off-link attackers from spoofing packets.
Bfd Authentication Enabled	When authentication is enabled.
Authentication type	Type of authentication: simple: Simple Password keyed-md5: Keyed message digest keyed-sha1: Keyed Secure hashing algorithm meticulous-keyed-md5: Meticulous Keyed message digest meticulous-keyed-sha1: Meticulous Keyed Secure hashing algorithm
Authentication Key-id	ID number of the authentication key.
Pkt In	Number of packets that have been received during this BFD session.
Pkt Out	Number of packets that have been transmitted during this BFD session.
Echo Out	Number of Echo-packets that have been transmitted during this BFD session.
IPv6 Pkt In	Number of IPv6 packets that have been received during this BFD session.
IPv6 Pkt Out	Number of IPv6 packets that have been transmitted during this BFD session.
UP Count	Number of times the BFD session has been up.
UPTIME	Length of time this BFD session has been up.
BGP-> Client ID	Protocol and module ID number of this BFD session’s neighboring device.
Flags	Session state of the neighboring device.
Interface	The interface on which the VRF resides.
Down-Reason	The reason causing the VRF to be down.

show bfd session A.B.C.D

Use this command to display information about an IPv4 BFD session neighbor.

Command Syntax

```
show bfd session A.B.C.D A.B.C.D (detail|)
show bfd session vrf WORD A.B.C.D A.B.C.D (detail|)
show bfd session A.B.C.D A.B.C.D <0-4294967295> (detail|)
show bfd session vrf WORD A.B.C.D A.B.C.D <0-4294967295> (detail|)
```

Parameters

WORD	Name of a specific Virtual Routing and Forwarding instance
A.B.C.D	Display the local IPv4 address.
A.B.C.D	Display the neighbor IPv4 address.
<0-4294967295>	Display the interface index of the address.
detail	Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 10.1.1.66 10.1.1.67 3
Session Interface Index: 3     Session Index: 1
Lower Layer: IPv4     Single Hop
Session State: Up
Local Discriminator: 1 Remote Discriminator: 163
Local Address: 10.1.1.66/32    Remote Address: 10.1.1.67/32
Local Port: 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4
UP Count: 1 UPTIME: 00:10:08


#show bfd session vrf raj 130.1.1.1 130.1.1.2 detail

Session Interface Index : 10017          Interface name :xe16
Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 130.1.1.1/32
Remote Discriminator : 2                 Remote Address : 130.1.1.2/32
Local Port : 49153                       Remote Port : 3784
Options :
```

```
    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250               Min Rx: 250               Multiplier: 3
    Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Sess Down Reason : NA
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : n/a                                  Pkt Out : n/a
    Pkts Drop : 00000000000000000000              Auth Pkts Drop :
    00000000000000000000
    Echo Out : 00000000000000000000               IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 00000000000000000000            IPv6 Pkt Out : 00000000000000000000
    UP Count : 1                                  UPTIME : 00:01:38

    Protocol Client Info:
    OSPF-> Client ID: 4      Flags: 4
```

Table 1-70 explains the output fields.

Table 1-70: Show BFD session fields

Entry	Description
Session Interface Index	ID number of the Interface.
Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.
Local Address	Local address of the transmitting device.
Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.

Table 1-70: Show BFD session fields

Entry	Description
Min Rx	Minimum receive interval in milliseconds.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	The number of times the BFD session has been in up state.
UPTIME	The length of time this BFD session has been in the up state.

show bfd session ipv6

Use this command to display information about an IPv6 BFD session neighbor.

Command Syntax

```
show bfd session ipv6 X:X::X:X X:X::X:X (detail|)
show bfd session ipv6 vrf WORD X:X::X:X X:X::X:X (detail|)
show bfd session ipv6 X:X::X:X X:X::X:X <0-4294967295> (detail|)
show bfd session ipv6 vrf WORD X:X::X:X X:X::X:X <0-4294967295> (detail|)
```

Parameters

WORD	Name of a specific Virtual Routing and Forwarding instance
X:X::X:X	Display the local IPv6 address.
X:X::X:X	Display the neighbor IPv6 address.
<0-4294967295>	Display the interface index of the address.
detail	Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 2001::1222 2001::1223 3
Session Interface Index : 3     Session Index: 1
Lower Layer: IPv6     Single Hop
Session State : Up
Local Discriminator : 1 Remote Discriminator: 163
Local Address : 2001::1222/128    Remote Address: 2001::1223/128
Local Port : 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4
UP Count: 1 UPTIME: 00:06:03


#show bfd session ipv6 vrf raj fe80::ba6a:97ff:fed3:26c5
fe80::ba6a:97ff:fece:3bc5 detail

Session Interface Index : 10017          Interface name :xe16
Session Index : 259
Lower Layer : IPv6                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 259                Local Address :
fe80::ba6a:97ff:fed3:26
c5/128
```

```
Remote Discriminator : 257              Remote Address :
fe80::ba6a:97ff:fece:3
bc5/128
Local Port : 49152                      Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 250             Neg Rx: 250             Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                                    Pkt Out : n/a
Pkts Drop : 00000000000000000000                Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000                 IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000001671              IPv6 Pkt Out : 00000000000000001675
UP Count : 1                                    UPTIME : 00:06:05

Protocol Client Info:
OSPF6-> Client ID: 5     Flags: 4
```

Table 1-71 explains the output fields.

Table 1-71: show BFD session fields

Entry	Description
Session Interface Index	ID number of the Interface.
Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Session Type	Whether the session is Single Hop or Multiple Hop
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.

Table 1-71: show BFD session fields

Entry	Description
Local Address	Local address of the transmitting device.
Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.
Min Rx	Minimum receive interval in milliseconds.
Min echo Tx	Minimum transmit interval for echo packets
Min echo Rx	minimum receive interval for echo packets
Neg echo intrvl	The negotiated
Storage type	Indicates the storage type: 1 = other 2 = volatile 3 = nonvolatile 4 = permanent 5 = read only
Sess down time	How long the session was down
Sess Down Reason	Reason for Session being down
Bfd GTSM	Whether Generalized TTL Security Mechanism (GTSM) is enabled or disabled on the connection.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	Number of times the BFD session has been in up state.
UPTIME	Length of time this BFD session has been in the up state.
Bfd Authentication	If authentication is used, if yes, the type authentication: simple password, MD5, and so on.
Pkt In	Number of Packets received on the BFD session
Pkt Out	Number of packets transmitted on the BFD session
Pkts Drop	Number of packets dropped on the session
Auth Pkts Drop	Number of Authentication packets dropped
Echo Out	Number of Transmitted BFD Echo Packets
IPv6 Echo Out	Number of transmitted BFD Ipv6 Echo packets
IPv6 Pkt In	Number of received IPv6 BFD packets
IPv6 Pkt Out	Number of transmitted IPV6 BFD packets
Protocol Client Info	Client ID and flags

show debugging bfd

Use this command to display debugging information for BFD processes.

Command Syntax

```
show debugging bfd
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show debugging bfd
BFD debugging status:
BFD events debugging is on
BFD packet debugging is on
BFD ipc-error debugging is on
BFD ipc-event debugging is on
BFD session debugging is on
BFD nsm debugging is on
#
```

snmp restart bfd

Use this command to restart SNMP in Bidirectional Forwarding (BFD)

Command Syntax

```
snmp restart bfd
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart bfd
```

CHAPTER 2 Protocol Commands for BFD

The chapter describes the commands used to manage BFD functionality for OSPF, IS-IS and BGP.

area virtual-link

Use this command to enable the BFD option for a specified virtual-link neighbor.

Use the no form of the command to disable BFD on a virtual-link neighbor.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
```

Parameters

A.B.C.D	Indicate an area IP address
<0-429467295>	Indicate an area ID in integer format
virtual-link	Indicate a virtual link and its parameters
A.B.C.D	Indicate the IP address of the virtual link
fall-over	Indicate fall-over detection
bfd	Specify the Bidirectional Forwarding Detection (BFD)

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf
(config-router)#area 1 virtual-link 192.168.0.1 fall-over bfd
```

bfd all-interfaces

Use this command to enable BFD for all neighbors maintained by an OSPF process or an ISIS instance.

Use the no form of the command to disable BFD.

Note: This command does not apply BFD to virtual-link neighbors.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

By default, bfd all interface is disabled

Command Mode

Configure router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf
(config-router)#bfd all-interfaces

#configure terminal
(config)#router isis
(config-router)#bfd all-interfaces
```

debug bgp bfd

Use this command to debug BFD processes in BGP.

Use the no form of the command to stop debugging.

Command Syntax

```
debug bgp bfd
no debug bgp bfd
undebug bgp bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug bgp bfd
```

debug isis bfd

Use this command to debug BFD processes in IS-IS.

Use the no form of the command to stop debugging.

Command Syntax

```
debug isis bfd
no debug isis bfd
undebug isis bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug isis bfd
```

debug ospf bfd

Use this command to debug BFD processes in OSPF.

Use the no form of the command to stop debugging.

Command Syntax

```
debug ospf bfd
no debug ospf bfd
undebug ospf bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ospf bfd
```

ip ospf bfd

Use this command to enable the BFD option for OSPF neighbors on an interface. Use the no form of the command to disable the BFD option for OSPF neighbors on an interface.

Note: When BFD monitoring is enabled for ospf session, protocol admin events like clear/ shutdown will cause BFD session to go to admin down.Due to this, neigbourship/adjacency down detection on peer will be according to the protocol configured dead interval and is not based on BFD interval.

Command Syntax

```
ip ospf bfd (disable|)
no ip ospf bfd (disable|)
```

Parameter

disable	Disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf bfd
```

isis bfd

Use this command to enable the BFD option for IS-IS neighbors on an interface. Use the no form of the command to disable the BFD option for neighbors on an interface.

Note: When BFD monitoring is enabled for ISIS session, protocol admin events like clear/ shutdown will cause BFD session to go to admin down. Due to this, neigbourship/adjacency down detection on peer will be according to the protocol configured hello hold interval and is not based on BFD interval.

Command Syntax

```
isis bfd (disable|)
no isis bfd (disable|)
```

Parameter

disable	Used to disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis bfd disable
```

CHAPTER 3 BFD Static Route Commands

Bidirectional Forwarding Detection (BFD) support for static routes can be configured on a static route basis, interface basis, or on a global level:

- When BFD is configured for an IPv4 or IPv6 static route, BFD provides the next-hop reachability detection for the given static route.
- When BFD is configured for an interface, BFD provides the data plane next-hop reachability information for any IPv4 or IPv6 static route configured through the given interface.
- When BFD is configured globally, BFD is applied on all interfaces with a single command. In all these cases, the BFD session update for NSM governs the state of the static routes.

This chapter includes the following commands:

ip bfd static all-interfaces

Use this command to enable BFD support for IPv4 static routes configured on all interfaces.

Use the no option with this command to disable BFD support for IPv4 static routes configured on all interfaces.

Command Syntax

```
ip bfd static all-interfaces
ip bfd vrf NAME static all-interfaces
no ip bfd static all-interfaces
no ip bfd vrf NAME static all-interfaces
```

Parameters

NAME	Enable/disable IPv4 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ip bfd static all-interfaces

#configure terminal
(config)#ip  bfd  vrf vrf1 static all-interfaces
```

ip static fall-over bfd

Use this command to enable BFD support for a specific IPv4 static route.

Use the no form of the command to disable the BFD support for a specific IPv4 static route.

Command Syntax

```
ip static A.B.C.D/M A.B.C.D fall-over bfd (disable|)
ip static vrf NAME A.B.C.D/M A.B.C.D fall-over bfd (disable|)
no ip static A.B.C.D/M A.B.C.D fall-over bfd (disable|)
ip static vrf NAME A.B.C.D/M A.B.C.D fall-over bfd (disable|)
```

Parameters

A.B.C.D/M	The IPv4 destination prefix and mask length.
A.B.C.D	The IPv4 gateway address.
disable	Disable BFD.
NAME	Enable/disable BFD for the IPv4 routes for this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ip static 4.4.4.4/32 20.0.10.82 fall-over bfd

#configure terminal
(config)# ip static vrf vrf1 4.4.4.4/32 20.0.10.82 fall-over bfd
```

ip static bfd

Use this command to enable or disable BFD support for IPv4 static route(s) configured on an interface.

Use the no option with this command to reset BFD support for IPv4 static route(s) configured on an interface.

Command Syntax

```
ip static bfd (disable|)
no ip static bfd (disable|)
```

Parameters

None

Command Mode

Interface mode

Default

By default, BFD static route support is disabled at all levels.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip static bfd disable

(config)#interface eth1
(config-if)#ip static bfd
```

ipv6 bfd static all-interfaces

Use this command to enable BFD support for IPv6 static routes on all interfaces.

Use the no option with this command to disable BFD support for IPv6 static routes on all interfaces.

Command Syntax

```
ipv6 bfd static all-interfaces
ipv6 bfd vrf NAME static all-interfaces
no ipv6 bfd static all-interfaces
no ipv6 bfd vrf NAME static all-interfaces
```

Parameters

NAME	Enable/disable IPv6 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ipv6 bfd static all-interfaces

#configure terminal
(config)#ipv6 bfd vrf vrf1 static all-interfaces
```

ipv6 static fall-over bfd

Use this command to enable BFD support for a specific IPv6 static route.

Use the no option with this command to disable BFD support for a specific IPv6 static route.

Command Syntax

```
ipv6 static X:X::X:X/M X:X::X:X fall-over bfd (disable|)
ipv6 static vrf NAME X:X::X:X/M X:X::X:X fall-over bfd (disable|)
no ipv6 static X:X::X:X/M X:X::X:X fall-over bfd (disable|)
no ipv6 static vrf NAME X:X::X:X/M X:X::X:X fall-over bfd (disable|)
```

Parameters

`X:X::X:X/M`	The IPv6 destination prefix and mask length.
`X:X::X:X`	The IPv6 gateway address.
`NAME`	Enable/disable BFD for the IPv6 routes for this user-defined Virtual Routing and Forwarding instance name.
`disable`	Disable BFD.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#ipv6 static 2345:6::0:1/28 2345:6::0:2 fall-over bfd

#configure terminal
(config)#ipv6 static 2345:12::1/64 2345:12::2 fall-over bfd disable

#configure terminal
(config)#ipv6 static vrf vrf1 2345:6::0:1/28 2345:6::0:2 fall-over bfd
```

ipv6 static bfd

Use this command to disable BFD support for IPv6 static route(s) configured on an interface.

Use the no option with this command to reset BFD support for IPv6 static route(s) configured on an interface.

Command Syntax

```
ipv6 static bfd (disable|)
no ipv6 static bfd (disable|)
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 static bfd disable
```

SECTION 12 Precision Time Protocol

Precision Time Protocol Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Boundary Clock Configuration

This chapter shows how to configure a boundary clock over Ethernet, IPv4, and IPv6. You configure a boundary clock with more than one port.

Note: We can enable PTP on physical interfaces which can be L2, L3 or member port of the LAG.

Topology

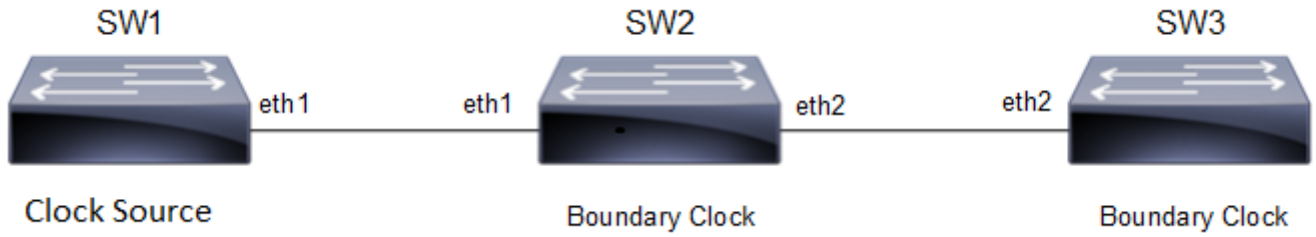


Figure 1-113: Configuration Topology

In this example, SW2 and SW3 are running PTP acting as boundary clock.

Boundary Clock Configuration

This section shows how to set up a boundary clock.

SW2 (boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#bridge 1 protocol mstp`	Create bridge 1 as an MSTP bridge (this step is not mandatory, but is a good practice to avoid layer 2 loops)
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)# mode synchronous`	Configure synchronous mode.
`(config-if-synce)#input-source 2`	Configure the interface as an input source with priority 2.
`(config-if-synce)#exit`	Exit Port Configure mode
`(conig-if)#exit`	Exit Interface mode
`(config)#interface eth2`	Configure interface eth2
`(config-if)#switchport`	Configure eth2 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth2 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.

(config-if-synce)#mode synchronous	Configure synchronous mode.
(config-if-synce)#output-source	Configure the interface as an output source.
(config-if-synce)#exit	Exit Port Configure mode
(config-if)#exit	Exit interface mode
(config)#ptp clock profile g8275.1	Enables G8275.1 for PTP time/phase telecom profile
(config-ptp-clk)#number-ports 2	Configure the number of PTP ports on the instance
(config-ptp-clk)#clock-port 2	Configure ptp port
(config-clk-port)#network-interface xe2	Configure underlying interface that is used by this PTP Port
(config-clk-port)#exit	Exit ptp clock port mode
(config-ptp-clk)#clock-port 1	Configure ptp port
(config-clk-port)#network-interface xe1	Configure underlying interface that is used by this PTP Port
(config-clk-port)#exit	Exit ptp clock port mode

SW3 (Boundary clock)

#configure terminal	Enter Configure mode
(config)#bridge 1 protocol mstp	Create bridge 1 as an MSTP bridge (this step is not mandatory, but is a good practice to avoid layer 2 loops)
(config)#synce	Enter configure Synchronous Ethernet mode.
(config-synce)#synchronization option 1	Set the synchronization network type.
(config-synce)#exit	Exit Synce mode
(config)#interface eth2	Configure interface eth2
(config-if)#switchport	Configure eth2 as Layer 2 port
(config-if)#bridge-group 1	Configure eth2 in bridge group 1
(config-if)#synce	Enter interface Synchronous Ethernet mode.
(config-if-synce)#mode synchronous	Configure synchronous mode.
(config-if-synce)#input-source 4	Configure the interface as an input source with priority 4.
(config-if-synce)#exit	Exit Port Configure mode
(config-if)#exit	Exit interface mode
(config)#ptp clock profile g8275.1	Enables G8275.1 for PTP time/phase telecom profile
(config-ptp-clk)#number-ports 2	Configure the number of PTP ports on the instance
(config-ptp-clk)#clock-port 2	Configure ptp port
(config-clk-port)#network-interface xe2	Configure underlying interface that is used by this PTP Port
(config-clk-port)#exit	Exit ptp clock port mode
(config-clk-clk)#clock-port 1	Configure ptp port
(config-clk-port)#network-interface xe1	Configure underlying interface that is used by this PTP Port
(config-clk-port)#exit	Exit ptp clock port mode

Validation

SW2

1. Verify the default data set on SW2.

```
#show ptp clock dataset default
Two Step Flag               : No
  Clock Identity              : B8:6A:97:FF:FE:F5:F4:C4
  Number Of Ports             : 2
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 24
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535
```

2. Verify the current data set on SW2.

```
#show ptp clock dataset current
Steps Removed               : 0
  Offset From Master          : 0 (0.000 nsec)
  Mean Path Delay             : 0
```

3. Verify the parent data set on SW2.

```
#show ptp clock dataset paren
Parent Port ID              :
    Clock Identity            : E8:C5:7A:FF:FE:2E:4B:1C
    Port Number               : 0
  Parent Stats                : No
  Observed Parent O.S.L.V     : 65535 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 2147483647 (Phase Change Rate)
  Grandmaster Identity        : E8:C5:7A:FF:FE:2E:4B:1C
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 248
    Clock Accuracy            : 38
    Offset ScaledLogVariance  : 65535
```

4. Verify the port state on SW2.

```
#show ptp port
Port 1:
  Port State                  : Slave
  Port Identity               : B8:6A:97:FF:FE:F5:F4:C4:00:01
  Log Min Delay Req Interval  : -4
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Announce Receipt Timeout    : 3
  Log Sync Interval           : -4
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
```

```
      Signal Fail                 : False
      Network Interface           : xe1
      Vlan Configured             :
      Description                 :

      Foreign Master #0
      L2 Address                  : e8:c5:7a:79:57:1d
      Grandmaster clockIdentity   : E8:C5:7A:FF:FE:2E:4B:1C
      Port ID                     : E8:C5:7A:FF:FE:2E:4B:1C:00:01
      clockClass                  : 135
      Clock accuracy              : 254
      Offset scaled log variance  : 65535
      priority1                   : 128
      priority2                   : 128
      Steps removed               : 0
      PDV Scaled Allan Variance   : 10

      Received Packets            : 7530
      Discarded Packets           : 4
      Transmitted Packets         : 3018

      Peer #0
      L2 Address                  : e8:c5:7a:79:57:1d
      Clock Identity              : e8:c5:7a:ff:fe:2e:4b:1c
      Received Announce           : 1021
      Received Sync               : 2042
      Received Delay Response     : 2041
      Transmitted Delay Request   : 2041

    Port 2:
      Port State                  : Master
      Port Identity               : B8:6A:97:FF:FE:F5:F4:C4:00:02
      Log Min Delay Req Interval  : -4
      Peer Mean Path Delay        : 0
      Log Announce Interval       : -3
      Announce Receipt Timeout    : 3
      Log Sync Interval           : -4
      Delay Mechanism             : End to end
      Version Number              : 2
      Local Priority              : 128
      Master only                 : False
      Signal Fail                 : False
      Network Interface           : xe2
      Vlan Configured             :
      Description                 :

      Received Packets            : 0
      Discarded Packets           : 0
      Transmitted Packets         : 113
```

Note: Use show `ptp stats` to collect the PTP statistics and use `clear ptp stats` to clear the same.

CHAPTER 2 PTP G.8275.1 Profile Configuration

This chapter shows how to configure a PTP G.8275.1 profile over Ethernet, IPv4, and IPv6. You configure T-GM and boundary clock with more than one port.

Note: We can enable G.8275.2 on L3 interfaces, sub interfaces and member port of the LAG.

Topology

Figure 2-114: Configuration Topology

In this example, SW1, SW2 and SW3 are running PTP. SW1 acting as T-GM and SW2, SW3 acting as boundary clock.

PTP G.8275.1 Profile Configuration

This section shows how to set up G.8275.1 profile.

SW2 (boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#bridge 1 protocol mstp`	Create bridge 1 as an MSTP bridge (this step is not mandatory, but is a good practice to avoid layer 2 loops)
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)# mode synchronous`	Configure synchronous mode.
`(config-if-synce)#input-source 2`	Configure the interface as an input source with priority 2.
`(config-if-synce)#exit`	Exit Port Configure mode
`(conig-if)#exit`	Exit Interface mode
`(config)#interface eth2`	Configure interface eth2
`(config-if)#switchport`	Configure eth2 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth2 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#output-source`	Configure the interface as an output source.
`(config-if-synce)#exit`	Exit Port Configure mode
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.1`	Enables G8275.1 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface eth1`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

SW3 (Boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#bridge 1 protocol mstp`	Create bridge 1 as an MSTP bridge (this step is not mandatory, but is a good practice to avoid layer 2 loops)
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#interface eth2`	Configure interface eth2
`(config-if)#switchport`	Configure eth2 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth2 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#input-source 4`	Configure the interface as an input source with priority 4.
`(config-if-synce)#exit`	Exit Port Configure mode
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.1`	Enables G8275.1 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 1`	Configure the number of PTP ports on the instance
`(config-clk-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

SW1 (T-GM)

`#configure terminal`	Enter Configure mode
`(config)#bridge 1 protocol mstp`	Create bridge 1 as an MSTP bridge (this step is not mandatory, but is a good practice to avoid layer 2 loops)
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface gps`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# mode synchronous`	Configure synchronous mode.
`(config-synce-if)# wait-to-restore 1`	Configure Wait-to-Restore timer.
`(config-synce-if)#exit`	Exit Port Configure mode
`(config)#interface eth1`	Configure interface eth2
`(config-if)#switchport`	Configure eth2 as Layer 2 port
`(config-if)#bridge-group 1`	Configure eth2 in bridge group 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#output-source`	Configure the interface as an output source.
`(config-if-synce)#exit`	Exit Port Configure mode
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.1`	Enables G8275.1 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)# master-only`	Configure the port as an master-only port
`(config-clk-port)#network-interface eth1`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface gps`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

Validation

SW2

1. Verify the default data set on SW2.

```
sh ptp clock dataset default
Two Step Flag               : No
```

```
  Clock Identity              : E8:C5:7A:FF:FE:23:6E:1C
  Number Of Ports             : 2
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 24
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535
```

2. Verify the current data set on SW2.

```
BC#sh ptp clock dataset current
  Steps Removed               : 1
  Offset From Master          : -25657344 (-391.500 nsec)
  Mean Path Delay             : 3449
```

3. Verify the parent data set on SW2.

```
BC# show ptp clock dataset parent
  Parent Port ID              :
    Clock Identity            : 00:00:00:00:00:00:00:01
    Port Number               : 1
  Parent Stats                : No
  Observed Parent O.S.L.V     : 0 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 0 (Phase Change Rate)
  Grandmaster Identity        : 00:00:00:00:00:00:00:01
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 6
    Clock Accuracy            : 33
    Offset ScaledLogVariance  : 65535
```

4. Verify the port state on SW2.

```
BC#sh ptp port
Port 1:
  Port State                  : Slave
  Port Identity               : E8:C5:7A:FF:FE:23:6E:1C:00:01
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Log Min Delay Req Interval  : -4
  Log Sync Interval           : -4
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : eth1
```

```
  Vlan Configured             :
  Description                 :
  Configured delay asymmetry  : 0 nsec

  Number of Foreign Masters   : 1
  Current Foreign Master      : 0

  Foreign Master #0
  L2 Address                  : a0:00:00:00:00:01
  Grandmaster clockIdentity   : 00:00:00:00:00:00:00:01
  Port ID                     : 00:00:00:00:00:00:00:01:00:01
  clockClass                  : 6
  Clock accuracy              : 33
  Offset scaled log variance  : 65535
  priority1                   : 128
  priority2                   : 128
  Steps removed               : 0
  PDV Scaled Allan Variance   : 5

  Received Packets            : 46955
  Discarded Packets           : 4
  Transmitted Packets         : 19485

  Drop Counters
  Pkt rcvd on bad port state  : 4

  Peer #0
  L2 Address                  : a0:00:00:00:00:01
  Clock Identity              : 00:00:00:00:00:00:00:01
  Received Announce           : 9392
  Received Sync               : 18784
  Received Delay Response     : 18781
  Transmitted Delay Request   : 18781

Port 2:
  Port State                  : Master
  Port Identity               : E8:C5:7A:FF:FE:23:6E:1C:00:02
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Log Min Delay Req Interval  : -4
  Log Sync Interval           : -4
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : eth2
  Vlan Configured             :
  Description                 :
```

```
  Configured delay asymmetry  : 0 nsec

  Received Packets            : 18783
  Discarded Packets           : 0
  Transmitted Packets         : 47655

  Peer #0
  L2 Address                  : d0:00:00:00:00:01
  Clock Identity              : 00:00:00:00:00:00:00:02
  Received Delay Request      : 18786
  Transmitted Announce        : 9626
  Transmitted Sync            : 19251
  Transmitted Delay Response  : 18786
```

5. Verify the ptp servo on SW2.

```
BC# sh ptp servo
PTP servo status for clock 0
  Servo Config                : Phase Correction
  Servo State                 : Normal Loop
  Servo State Duration        : 00:20:46
  Servo APTS Mode             : N/A
  Frequency Correction        : 0.000 ppb
  Phase Correction            : -3537.000 nsec
  Offset From Master          : -479.000 nsec
  Mean Path Delay             : 3536 nsec
  APTS GPS to PTP Offset      : 0 nsec
  Sync Packet Rate            : 16
  Delay Packet Rate           : 16
```

Note: Use show ptp stats to collect the PTP statistics and use clear ptp stats to clear the same.

CHAPTER 3 PTP G.8275.2 Profile Configuration

This chapter shows how to configure a PTP G.8275.2 profile over IPv4 and IPv6. You configure T-GM and boundary clock with more than one port.

Note: We can enable G.8275.2 on L3 interfaces, sub interfaces and member port of the LAG.

Partial Timing Support (PTS) Topology

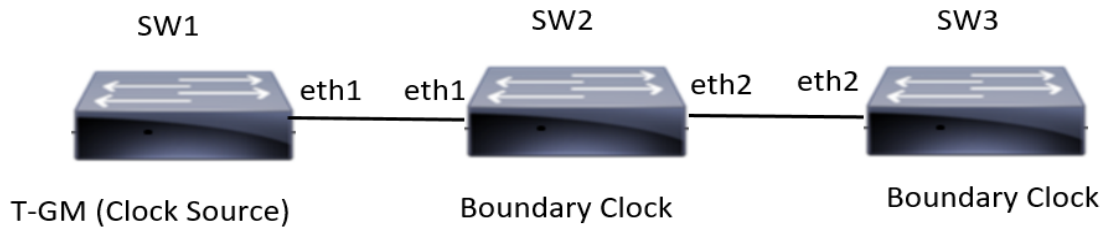


Figure 3-115: Configuration Topology

In this example, SW1, SW2 and SW3 are running PTP. SW1 acting as T-GM and SW2, SW3 acting as boundary clock.

PTS G.8275.2 Profile Configuration

This section shows how to set up a G.8275.2 Profile.

SW2 (boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface ptp`	Configure synce interface ptp
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)# interface eth1`	Configure interface eth1
`(config-if)# ip address 192.168.4.101/24`	Configure the IP address of the interface.
`(config-synce-if)# exit`	Exit synce Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)# ip address 192.168.5.100/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)# transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth1`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#master ipv4 192.168.4.100`	Set master clock source address
`(config-clk-port)# exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)#transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

SW3 (Boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface ptp`	Configure synce interface ptp
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)# interface eth1`	Configure interface eth1
`(config-if)# ip address 192.168.4.101/24`	Configure the IP address of the interface.
`(config-synce-if)# exit`	Exit synce Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)# ip address 192.168.5.100/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)# transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth1`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#master ipv4 192.168.4.100`	Set master clock source address
`(config-clk-port)# exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)#transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

SW1 (T-GM)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface gps`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# wait-to-restore 1`	Configure Wait-to-Restore timer.
`(config-synce-if)#exit`	Exit Port Configure mode
`(config)#synce-interface ptp`	Configure synce interface ptp
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 2`	Configure the interface as an input source with priority 2
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)#ip address 192.168.4.100/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)# transport ipv4`	Configure the port as an master-only port
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)# master-only`	Configure the port as an master-only port
`(config-clk-port)#exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface gps`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

Validation

SW2

1. Verify the default data set on SW2.

```
# BC#show ptp clock dataset default
  Two Step Flag               : No
  Clock Identity              : E8:C5:7A:FF:FE:02:A0:3C
  Number Of Ports             : 2
```

```
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 44
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535
```

2. Verify the current data set on SW2.

```
# show ptp clock dataset current
  Steps Removed               : 1
  Offset From Master          : -131072 (-2.000 nsec)
  Mean Path Delay             : 3060
```

3. Verify the parent data set on SW2.

```
# show ptp clock dataset parent
  Parent Port ID              :
    Clock Identity            : 00:00:00:00:00:00:00:01
    Port Number               : 1
  Parent Stats                : No
  Observed Parent O.S.L.V     : 0 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 0 (Phase Change Rate)
  Grandmaster Identity        : 00:00:00:00:00:00:00:01
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 6
    Clock Accuracy            : 33
    Offset ScaledLogVariance  : 20061
```

4. 4. Verify the port state on SW2.

```
# sh ptp port
Port 1:
  Port State                  : Slave
  Port Identity               : E8:C5:7A:FF:FE:02:A0:3C:00:01
  Log Min Delay Req Interval  : -6
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Announce Receipt Timeout    : 3
  Log Sync Interval           : -6
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
```

```
  Network Interface           : eth1
  Vlan Configured             :
  Description                 :
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300

  Number of Foreign Masters   : 1
  Current Foreign Master      : 0

  Foreign Master #0
  IPv4 Address                : 192.168.4.100
  Grandmaster clockIdentity   : 00:00:00:00:00:00:00:01
  Port ID                     : 00:00:00:00:00:00:00:01:00:01
  clockClass                  : 6
  Clock accuracy              : 33
  Offset scaled log variance  : 20061
  priority1                   : 128
  priority2                   : 128
  Steps removed               : 0
  PDV Scaled Allan Variance   : 5

  Received Packets            : 109666
  Discarded Packets           : 0
  Transmitted Packets         : 51821

  Peer #0
  IPv4 Address                : 192.168.4.100
  Clock Identity              : 00:00:00:00:00:00:00:01
  Received Announce           : 6435
  Received Sync               : 51415
  Received Delay Response     : 51825
  Received Signalling         : 18
  Transmitted Delay Request   : 51825
  Transmitted Signalling      : 38

  Master #0                   : 192.168.4.100

Port 2:
  Port State                  : Master
  Port Identity               : E8:C5:7A:FF:FE:02:A0:3C:00:02
  Log Min Delay Req Interval  : -6
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Announce Receipt Timeout    : 3
  Log Sync Interval           : -6
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
```

```
  Signal Fail                 : False
  Network Interface           : eth2
  Vlan Configured             :
  Description                 :
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300

  Received Packets            : 51476
  Discarded Packets           : 0
  Transmitted Packets         : 109804

  Peer #0
  IPv4 Address                : 192.168.5.101
  Clock Identity              : 00:00:00:00:00:00:00:02
  Received Delay Request      : 51485
  Received Signalling         : 18
  Transmitted Announce        : 6436
  Transmitted Sync            : 51902
  Transmitted Delay Response  : 51485
  Transmitted Signalling      : 18

  Slave #0
  IPv4 Address                : 192.168.5.101
  Clock Identity              : 00:00:00:00:00:00:00:02
  Delay Mechanism             : End to end
  log Announce Interval       : -3
  log Sync Interval           : -6
  Log Delay Req Interval      : -6
```

5. Verify the ptp servo on SW2.

```
# sh ptp servo
PTP servo status for clock 0
  Servo Config                : Freq + Phase Correction
  Servo State                 : Time Locked
  Servo State Duration        : 00:13:33
  Servo APTS Mode             : PTP
  Frequency Correction        : -0.674 ppb
  Phase Correction            : 0.000 nsec
  Offset From Master          : 10.000 nsec
  Mean Path Delay             : 3060 nsec
  APTS GPS to PTP Offset      : 0 nsec
  Sync Packet Rate            : 64
  Delay Packet Rate           : 65
```

Note: Use show ptp stats to collect the PTP statistics and use clear ptp stats to clear the same.

Asserted Partial Timing Support (APTS) Topology

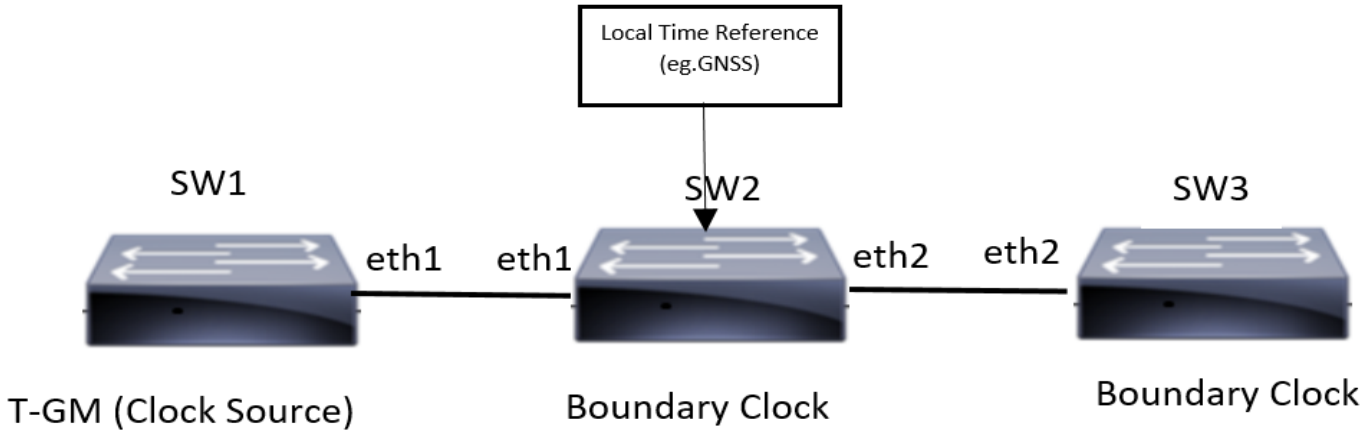


Figure 3-116: Configuration Topology

In this example, SW1, SW2 and SW3 are running PTP. SW1 acting as T-GM and SW2, SW3 acting as boundary clock.

APTS G.8275.2 Profile Configuration

This section shows how to set up a G.8275.2 Profile.

SW2 (boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface gps`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# wait-to-restore 1`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)#synce-interface ptp`	Configure synce interface ptp
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 2`	Configure the interface as an input source with priority 2
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)# interface eth1`	Configure interface eth1
`(config-if)# ip address 192.168.4.101/24`	Configure the IP address of the interface.
`(config-synce-if)# exit`	Exit synce Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)# ip address 192.168.5.100/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 3`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface gps`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)# transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth1`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#master ipv4 192.168.4.100`	Set master clock source address
`(config-clk-port)# exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 3`	Configure ptp port
`(config-clk-port)#transport ipv4`	Set transport type ipv4
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

SW3 (Boundary clock)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface ptp`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)#ip address 192.168.5.101/24`	Configure eth2 as Layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 1`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#transport ipv4`	Set transport type ipv4.
`(config-clk-port)#master ipv4 192.168.5.100`	Set master clock source address.
`(config-clk-port)#exit`	Exit ptp clock port mode

SW1 (T-GM)

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode
`(config)#synce-interface gps`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# input-source 1`	Configure the interface as an input source with priority 1
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# wait-to-restore 1`	Configure Wait-to-Restore timer.
`(config-synce-if)#exit`	Exit Port Configure mode
`(config)#synce-interface ptp`	Configure synce interface gps
`(config-synce-if)# mode synchronous`	Configure synchronous mode
`(config-synce-if)# quality-level QL_PRC`	Configure QL-value.
`(config-synce-if)# input-source 2`	Configure the interface as an input source with priority 2
`(config-synce-if)# wait-to-restore 0`	Configure Wait-to-Restore timer.
`(config-synce-if)# exit`	Exit Port Configure mode.
`(config)#interface eth2`	Configure interface eth2
`(config-if)#ip address 192.168.4.100/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode
`(config)#ptp clock profile g8275.2`	Enables G8275.2 for PTP time/phase telecom profile
`(config-ptp-clk)#number-ports 2`	Configure the number of PTP ports on the instance
`(config-ptp-clk)#clock-port 2`	Configure ptp port
`(config-clk-port)# transport ipv4`	Configure the port as an master-only port
`(config-clk-port)#network-interface eth2`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)# master-only`	Configure the port as an master-only port
`(config-clk-port)#exit`	Exit ptp clock port mode
`(config-ptp-clk)#clock-port 1`	Configure ptp port
`(config-clk-port)#network-interface gps`	Configure underlying interface that is used by this PTP Port
`(config-clk-port)#exit`	Exit ptp clock port mode

Validation

SW2

1. Verify the default data set on SW2.

```
BC# show ptp clock dataset default
  Two Step Flag               : No
  Clock Identity              : E8:C5:7A:FF:FE:23:6E:1C
  Number Of Ports             : 3
  Priority1                   : 128
  Priority2                   : 128
```

```
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 44
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535
```

2. Verify the current data set on SW2.

```
BC#show ptp clock dataset current
  Steps Removed               : 1
  Offset From Master          : 0 (0.000 nsec)
  Mean Path Delay             : 0
```

3. Verify the parent data set on SW2.

```
BC#show ptp clock dataset parent
  Parent Port ID              :
    Clock Identity            : 00:00:00:00:00:00:00:01
    Port Number               : 1
  Parent Stats                : No
  Observed Parent O.S.L.V     : 0 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 0 (Phase Change Rate)
  Grandmaster Identity        : 00:00:00:00:00:00:00:01
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 6
    Clock Accuracy            : 33
    Offset ScaledLogVariance  : 20061
```

4. Verify the port state on SW2.

```
BC#sh ptp port
Port 1:
  Port State                  : Slave
  Port Identity               : E8:C5:7A:FF:FE:23:6E:1C:00:01
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Log Min Delay Req Interval  : 127
  Log Sync Interval           : -6
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 0
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : gps
  Vlan Configured             :
  Description                 :
```

```
  TTL                          : 64
  DSCP                         : 56
  Unicast Grant Duration       : 300
  Configured delay asymmetry   : 0 nsec

  Received Packets             : 0
  Discarded Packets            : 0
  Transmitted Packets          : 0

Port 2:
  Port State                   : Slave
  Port Identity                : E8:C5:7A:FF:FE:23:6E:1C:00:02
  Peer Mean Path Delay         : 0
  Log Announce Interval        : -3
  Log Min Delay Req Interval   : -6
  Log Sync Interval            : -6
  Announce Receipt Timeout     : 3
  Delay Mechanism              : End to end
  Version Number               : 2
  Local Priority               : 128
  Master only                  : False
  Signal Fail                  : False
  Network Interface            : xe14
  Vlan Configured              :
  Description                  :
  TTL                          : 64
  DSCP                         : 56
  Unicast Grant Duration       : 300
  Configured delay asymmetry   : 0 nsec

  Number of Foreign Masters    : 1
  Current Foreign Master       : 0

  Foreign Master #0
  IPv4 Address                 : 192.168.4.100
  Grandmaster clockIdentity    : 00:00:00:00:00:00:00:01
  Port ID                      : 00:00:00:00:00:00:00:01:00:02
  clockClass                   : 6
  Clock accuracy               : 33
  Offset scaled log variance   : 20061
  priority1                    : 128
  priority2                    : 128
  Steps removed                : 0
  PDV Scaled Allan Variance    : 32

  Received Packets             : 41218
  Discarded Packets            : 0
  Transmitted Packets          : 19473

  Peer #0
```

```
  IPv4 Address                : 192.168.4.100
  Clock Identity              : 00:00:00:00:00:00:00:01
  Received Announce           : 191
  Received Sync               : 1523
  Received Delay Response     : 1536
  Transmitted Delay Request   : 1536

  Master #0                   : 192.168.4.100

Port 3:
  Port State                  : Master
  Port Identity               : E8:C5:7A:FF:FE:23:6E:1C:00:03
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Log Min Delay Req Interval  : -6
  Log Sync Interval           : -6
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : xe15
  Vlan Configured             :
  Description                 :
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300
  Configured delay asymmetry  : 0 nsec

  Received Packets            : 19385
  Discarded Packets           : 0
  Transmitted Packets         : 41355

  Peer #0
  IPv4 Address                : 192.168.5.101
  Clock Identity              : 00:00:00:00:00:00:00:02
  Received Delay Request      : 1521
  Received Signalling         : 3
  Transmitted Announce        : 190
  Transmitted Sync            : 1533
  Transmitted Delay Response  : 1521
  Transmitted Signalling      : 3

  Slave #0
  IPv4 Address                : 192.168.5.101
  Clock Identity              : 00:00:00:00:00:00:00:02
  Delay Mechanism             : End to end
  log Announce Interval       : -3
  log Sync Interval           : -6
```

```
  Log Delay Req Interval      : -6
```

5. Verify the ptp servo on SW2.

```
BC# sh ptp servo
PTP servo status for clock 0
  Servo Config                : Freq + Phase Correction
  Servo State                 : Time Locked
  Servo State Duration        : 00:11:17
  Servo APTS Mode             : GPS
  Frequency Correction        : 0.002 ppb
  Phase Correction            : 0.000 nsec
  Offset From Master          : 0.000 nsec
  Mean Path Delay             : 0 nsec
  APTS GPS to PTP Offset      : 32723445187 nsec
  Sync Packet Rate            : 0
  Delay Packet Rate           : 0
```

Note: Use show ptp stats to collect the PTP statistics and use clear ptp stats to clear the same.

Precision Time Protocol Command Reference

Contents

This document contains these chapters:

CHAPTER 1 PTP 8275.1 and PTP 8275.2 Commands

This chapter contains the configuration commands used for Precision Time Protocol (PTP). It includes the following commands:

- show ptp servo history
- slave-only
- show ptp stats
- slave-only
- source-address
- Transport
- ttl
- unicast-grant-duration

1pps-out offset

Use this command to set 1PPS external interface output signal offset in nano seconds.

Use no form of this command to set default value 0.

Command Syntax

```
1pps-out offset <-2048-2048>
no 1pps-out offset
```

Parameters

<-2048-2048>	Offset value in range. Default is 0

Command Mode

PTP Clock Mode

Default

Default offset value is Zero.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#ptp clock profile g8275.1
OcNOS(config-ptp-clk)#1pps-out offset ?
  <-2048-2048>  Offset value in range. Default is 0
(config-ptp-clk)#1pps-out offset 2048
```

announce-receipt-timeout

Use this command to set announce-receipt-timeout. Applicable for only G.8275.2 profile.

Use no form of this command to set default value 3.

Command Syntax

```
announce-receipt-timeout <2-10>
no announce-receipt-timeout
```

Parameters

<2-10>	announceReceiptTimeout range (default is 3)

Command Mode

PTP Clock Port Mode

Default

Default offset value is Zero.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#announce-receipt-timeout 3
```

clear ptp stats

Use this command to clear PTP packet statistics.

Command Syntax

```
clear ptp stats
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

.Example

```
#clear ptp stats
```

clock-accuracy

Use this command to indicate the expected accuracy of the clock.

Note: Applicable for Non-Ethernet ports for PTP Clock Port mode.

Command Syntax

```
clock-accuracy <0-255>
no clock-accuracy
```

Parameters

<0-255>	A number representing the expected clock accuracy.

Command Mode

PTP Clock Mode and PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-accuracy 10
```

Note: Use no form of this command in PTP Clock Mode to set default value 254.

```
(config-ptp-clk)#clock-port 1
(config-clk-port)#clock-accuracy 15
```

Note: Use no form of this command in PTP Clock Port Mode to set default value 0x21.

clock-class

Use this command to denote the traceability of the time or frequency distributed by the clock.

Note: Applicable for Non-Ethernet ports for PTP Clock Port mode.

Command Syntax

```
clock-class <0-255>
no clock-class
```

Parameters

<0-255>	A number representing the traceability of time or frequency of the clock.

Command Mode

PTP Clock Mode and PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-class 3
```

Note: Use no form of this command in PTP Clock Mode to set default value 248.

```
(config-ptp-clk)#clock-port 1
(config-clk-port)#clock-class 7
```

Note: Use no form of this command in PTP Clock Port Mode to set default value 6 for clock-port.

clock-port

Use this command to enter PTP Clock Mode. To remove the clock-port configuration, use the no form of the command.

Command Syntax

```
clock-port <1-31>
no clock-port <1-31>
```

Parameters

<1-32>	Port number

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#
```

delay-asymmetry

Use this command to set asymmetric delay in nanoseconds.

Use no form of this command to set default value 0.

Command Syntax

```
delay-asymmetry {msec <-100-100>|nsec <-1000000-1000000>}
no delay-asymmetry
```

Parameters

`msec <-100-100>`	Value of latency in msec.
`nsec<-1000000-1000000>`	Value of latency in nsec.

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.End with CNTL/Z. (config)#
(config)#ptp clock profile g8275.2 (config-ptp-clk)#clock-port 1
(config-clk-port)# delay-asymmetry msec 100 nsec 1000000
```

description

Use this command to set description for clock port.

Use no form of this command to delete this description.

Command Syntax

```
description LINE
no description
```

Parameters

LINE	Characters describing this clock port.

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#description l3
```

domain

Use this command to set the current synchronization domain. For the G.8275.1 profile, valid domain numbers are in the range of 24 - 43 and default is 24. For the G.8275.2 profile, valid domain numbers are in the range of 44 - 63 and default is 44.

Command Syntax

```
domain <24-63>
no domain
```

Parameters

<24-63>	A numerical value that represents a synchronization domain.

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#domain 30
```

dscp

Use this command to set dscp value. Applicable for g.8275.2 profile.

Use no form of this command to set default value 56.

Command Syntax

```
dscp <0-63>
no dscp
```

Parameters

`<0-63>` Setting dscp value (default is 56)

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#dscp 2
```

gps-offset

Use this command to set GPS offset in nano seconds ans seconds.

Use no form of this command to set default value 0 nsec.

Command Syntax

```
gps-offset (sec <-100-100> | nsec <-2048-2048>)
no gps-offset
```

Parameters

`sec <-100-100>`	Offset value in seconds.
`nsec<-2048-2048>`	Offset value in nano seconds.

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#gps-offset sec 100 nsec 2048
```

grandmaster-priority2

Use this command to set grandmaster-priority2 for virtual-clock-port. Applicable for g.8275.1 profile. Not applicable to Ethernet interfaces.

Use no form of this command to set priority2 default value 128.

Command Syntax

```
grandmaster-priority2 <0-255>
no grandmaster-priority2
```

Parameters

<0-255>	Priority range

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#grandmaster-priority2 2
```

holdover

Use this command to enable holdover.

Use no form of this command to set default duration 120.

Command Syntax

```
holdover <0-1440>
no holdover
```

Parameters

<0-1440>	Range of holdover in minutes.

Command Mode

PTP Clock Mode

Default

Default holdover minutes is 120.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#holdover 15
```

local-priority (ptp-clk mode)

Use this command to specify the local attribute of the local clock.

Use no form of this command to set default value 128.

Command Syntax

```
local-priority <1-255>
no local-priority
```

Parameters

<1-255>	A numerical value specifying the local priority

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#local-priority 100
```

local-priority (ptp-clk-port mode)

Use this command to specify the local attribute of the local clock.

Use no form of this command to set default value 128.

Command Syntax

```
local-priority <1-255>
no local-priority
```

Parameters

<1-255>	A numerical value specifying the local priority

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 5
(config-clk-port)#local-priority 50
```

log-announce-interval

Use this command to set log-announce-interval. Applicable for only G.8275.2 profile.

Use no form of this command to set default value -3.

Command Syntax

```
log-announce-interval <-3-0>
no log-announce-interval
```

Parameters

<-3-0>	logAnnounceInterval range (default is -3)

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#log-announce-interval -2
```

log-min-delay-req-interval

Use this command to set log-min-delay-req-interval. Applicable for only G.8275.2 profile.

Use `no` form of this command to set default value -6.

Command Syntax

```
log-min-delay-req-interval <-7-0>
no log-min-delay-req-interval
```

Parameters

`<-7-0>`	minDelayReqInterval range (default is -6)

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#log-min-delay-req-interval -5
```

log-sync-interval

Use this command to set log-sync-interval. Applicable for only G.8275.2 profile.

Use no form of this command to set default value -6.

Command Syntax

```
log-sync-interval <-7-0>
no log-sync-interval
```

Parameters

<-7-0>	logSyncInterval range (default is -6)

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#log-sync-interval -4
```

master

Use this command to configure master ipv4 and ipv6 address. Applicable for g.8275.2 profile.

Use no form of this command to delete master address.

Command Syntax

```
master (ipv4 A.B.C.D|ipv6 X:X::X:X)
no master (ipv4 A.B.C.D|ipv6 X:X::X:X)
```

Parameters

ipv4	Setting master ipv4 address
A.B.C.D	Setting ipv4 clock source
ipv6	Setting master ipv6 address
X:X::X:X	Setting ipv6 clock source

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#transport ipv4
(config-clk-port)#master ipv4 10.1.1.2
```

master-only

Use this command to set a port to a master-only port.

Use no form of this command to delete this configuration.

Command Syntax

```
master-only
no master-only
```

Parameters

None

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 10
(config-clk-port)#master-only
```

max-steps-removed

Use this command to specify the maximum number of communication paths between the local clock and the grandmaster clock.

Use no form of this command to set default value 255.

Command Syntax

```
max-steps-removed <1-255>
no max-steps-removed
```

Parameters

<1-255>	The number of communication links between the local clock and the grandmaster clock.

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
# configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#max-steps-removed 10
```

network-interface

Use this command to reference the configured underlying interface that is used by this PTP Port.

Use no form of this command to delete network-interface.

Command Syntax

```
network-interface  IFNAME
network-interface  IFNAME  vlan  VLAN_ID
network-interface  IFNAME  port  IFNAME
network-interface  (gps|prc)
no network-interface
```

Parameters

IFNAME	The name of a physical interface
gps	GPS interface
prc	SMA/SMB or external interfaces
Vlan	Vlan configuration applicable for g8275.1 profile
VLAN_ID	VLAN ID 1-4094
Port	Physical port

Command Mode

PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#clock-port 1
(config-clk-port)#network-interface xe2
(config-clk-port)#exit
(config-ptp-clk)#clock-port 2
(config-clk-port)#network-interface xe3 vlan 2
(config-clk-port)#exit
(config-ptp-clk)#clock-port 3
(config-clk-port)#network-interface gps
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#network-interface vlan1.2 port xe1
```

number-ports

Use this command to set the number of PTP ports on the instance. If the number of ports is larger than one, the clock is configured as a boundary clock, otherwise it's an ordinary clock.

Use no form of this command to set default value 1.

Command Syntax

```
number-ports <1-31>
no number-ports
```

Parameters

<1-31>	The number of PTP ports on this instance.

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#number-ports 3
```

offset-log-variance

Use the command to specify an offset variance. The offset (scaled logarithmic variance) provides an estimate of the variations of the clock from a linear time scale when it is not synchronized to another clock using the PTP protocol.

Note: Applicable for Non-Ethernet ports for PTP Clock Port mode.

Command Syntax

```
offset-log-variance <0-65535>
no offset-log-variance
```

Parameters

`<0-65535>`	The offset variance when not synchronized.

Command Mode

PTP Clock Mode and PTP Clock Port Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#offset-log-variance 3000
```

Note: Use no form of this command in PTP Clock Mode to set default value 65535.

```
(config-ptp-clk)#clock-port 1
(config-clk-port)#offset-log-variance 2000
```

Note: Use no form of this command in PTP Clock Port Mode to set default value 0x4E5D for clock-port.

priority2

Use this command to set the Priority2 attribute of the local clock (as specified in the IEEE-1588 standard).

Use no form of this command to set default value 128.

Command Syntax

```
priority2 <1-255>
no priority2
```

Parameters

<1-255>	The Priority2 attribute.

Command Modeg

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#priority2 3
```

ptp clock profile

Use this command to enter PTP Clock Mode and to configure the g8275.1 and g8275.2 profile.

Use no form of this command to delete ptp clock.

Command Syntax

```
ptp (clock) profile (g8275.1|g8275.2)
no ptp (clock) profile (g8275.1|g8275.2)
```

Parameters

g8275.1	PTP time/phase g8275.1 telecom profile
g8275.2	PTP time/phase g8275.2 telecom profile

Command Mode

PTP Clock Mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)exit

#configure terminal
 (config)#ptp clock profile g8275.2
 (config-ptp-clk)exit
```

reserved-vlan-base-id

Use this command to set the Reserved VLAN base ID.

Use no form of this command to set default base id 4064.

Command Syntax

```
reserved-vlan-base-id <2-4094>
no reserved-vlan-base-id
```

Parameters

<2-4094>	Base VLAN identifier range.

Command Mode

PTP Clock Mode

Default

Default VLAN base ID is 4064.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)#reserved-vlan-base-id 2
```

servo-history

Use this command to enable servo-history with specified interval.

Use no form of this command to disable servo-history.

Command Syntax

```
servo-history <1-60>
no servo-history
```

Parameters

<1-60>	Enable servo-history in interval of <1-60> mins (default is 15 mins)

Command Mode

PTP Clock Mode

Default

Default interval value is 15 mins.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.1
(config-ptp-clk)# servo-history 2
```

show ptp clock

Use this command to display a summary of the Precision Time Protocol (PTP) clock status.

Command Syntax

```
show ptp clock (dataset (default|current|parent|time-properties|)|)
```

Parameters

`dataset`	The clock dataset
`default`	The default clock status
`current`	The current clock status
`parent`	The clock status of the parent-clock
`time-properties`	The clock dataset time-properties

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ptp clock
PTP Clock Profile             : g8275.1
Holdover Duration             : 120 min
Default Dataset:
  Two Step Flag               : No
  Clock Identity              : B8:6A:97:FF:FE:F5:F4:C4
  Number Of Ports             : 1
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 24
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535

Current Dataset:
  Steps Removed               : 0
  Offset From Master          : 0 (0.000 nsec)
  Mean Path Delay             : 0

Parent Dataset:
  Parent Port ID              :
    Clock Identity            : B8:6A:97:FF:FE:F5:F4:C4
```

```
        Port Number               : 0
      Parent Stats                : No
      Observed Parent O.S.L.V     : 65535 (Offset Scaled Log Variance)
      Observed Parent P.C.R.      : 2147483647 (Phase Change Rate)
      Grandmaster Identity        : B8:6A:97:FF:FE:F5:F4:C4
      Grandmaster Priority1       : 128
      Grandmaster Priority2       : 128
      Grandmaster Clock Quality   :
        Clock Class               : 248
        Clock Accuracy            : 38
        Offset ScaledLogVariance  : 65535

    Time Dateset:
      Current UTC Offset Valid    : False
      Current UTC Offset          : 36
      Leap 59                     : False
      Leap 61                     : False
      Time Traceable              : False
      Frequency Traceable         : False
      PTP Timescale               : True
      Time Source                 : Internal Oscillator
      Time of Day                 : Thu Jan  1 19:52:59 1970
```

show ptp port brief

Use this command to display a summary of PTP ports.

Command Syntax

```
show ptp port brief
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show ptp port brief
Clock    Intf               Port                    Link
Port     Name               State          Encap    State     Mechanism
-------------------------------------------------------------------------
1        xe2                Master         Eth      Up        1-step E2E
2        xe1                Master         Eth      Up        1-step E2E
```

show ptp port dataset

Use this command to display a summary of PTP ports.

Command Syntax

```
show ptp port (<1-31>|) dataset
```

Parameters

<1-31>	PTP port number

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ptp port dataset
Port 1:
  Port State                  : Master
  Port Identity               : B8:6A:97:FF:FE:F5:F4:C4:00:01
  Log Min Delay Req Interval  : -4
  Peer Mean Path Delay        : 0
  Log Announce Interval       : -3
  Announce Receipt Timeout    : 3
  Log Sync Interval           : -4
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : xe0
  Vlan Configured             :
  Description                 : l3
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300
  Configured delay asymmetry  : 101000000 nsec
  Received Packets            : 0
  Discarded Packets           : 0
  Transmitted Packets         : 99
```

show ptp port peer

Use this command to display a peer summary of PTP ports.

Command Syntax

```
show ptp port (<1-31>|) peer
```

Parameters

<1-31>	PTP port number

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show ptp port peer
Port 1 (1 peers):
  Peer #0
  IPv4 Address                : 10.1.1.2
  Clock Identity              : e8:c5:7a:ff:fe:2e:63:1c
  Received Announce           : 3297
  Received Sync               : 26523
  Received Delay Response     : 26524
  Received Signalling         : 9
  Transmitted Delay Request   : 26524
  Transmitted Signalling      : 9
```

show ptp port master

Use this command to display a master summary of PTP ports.

Command Syntax

```
show ptp port (<1-31>|) master
```

Parameters

<1-31>	PTP port number

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ptp port master
Port 1:
  Master #0                   : 10.1.1.2
```

show ptp port slave

Use this command to display a slave summary of PTP ports.

Command Syntax

```
show ptp port (<1-31>|) slave
```

Parameters

<1-31>	PTP port number

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show ptp port slave
Port 1:  Slave #0
     IPv4 Address                : 10.1.1.1
    Clock Identity              : e8:c5:7a:ff:fe:2e:4b:1c
    Delay Mechanism             : End to end
    log Announce Interval       : -3
    log Sync Interval           : -6
    Log Delay Req Interval      : -6
```

show ptp servo

Use this command to display servo information.

Command Syntax

```
show ptp servo
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ptp servo
PTP servo status for clock 0
  Servo Config                : Phase Correction
  Servo State                 : Warmup
  Servo State Duration        : 04:26:07
  Servo APTS Mode             : N/A
  Lock Status                 : Unlocked
  Frequency Correction        : 0.000 ppb
  Phase Correction            : 0.000 nsec
  Offset From Master          : 0.000 nsec
  Mean Path Delay             : 0 nsec
  Sync Packet Rate            : 0
  Delay Packet Rate           : 0
```

show ptp servo history

Use this command to display servo history.

Command Syntax

```
show ptp servo history
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
# OcNOS#show ptp servo history
Time                            Phase Correction        Freq Correction
                                (nsec)                  (pbb)
-----------------------------------------------------------------------
2000 Jan 06 19:15:01            0.000                   0.000
2000 Jan 06 19:17:01            0.000                   0.000
2000 Jan 06 19:19:01            0.000                   0.000
2000 Jan 06 19:21:01            0.000                   0.000
2000 Jan 06 19:23:01            0.000                   0.000
2000 Jan 06 19:25:01            0.000                   0.000
```

show ptp stats

Use this command to display PTP packet statistics.

Command Syntax

```
show ptp stats
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ptp stats

clock 0:
  Number of ports             : 32
  Received Packets            : 0
  Discarded Packets           : 0
  Received IPv4 PTP Packets   : 0
  Received IPv6 PTP Packets   : 0
  Received L2 PTP Packets     : 0
  RX Queue Overflows          : 0
  Transmitted Packets         : 346

Port 1:
  Received Packets            : 0
  Discarded Packets           : 0
  Transmitted Packets         : 34
```

slave-only

Use this command to set a clock to a slave-only clock.

Use no form of this command to unconfigure this option.

Command Syntax

```
slave-only
no slave-only
```

Parameters

None

Command Mode

PTP Clock Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ptp clock profile g8275.1
(config-ptp-clk)#slave-only
```

source-address

Use this command to set source-address as linklocal for g.8275.2 profile.

Use no form of this command to unconfigure this command.

Command Syntax

```
source-address ipv6 linklocal
no source-address ipv6 linklocal
```

Parameters

None.

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)# source-address ipv6 linklocal
```

Transport

Use this command to set transport type as ipv4 or ipv6. Applicable for g.8275.2 profile.

Use no form of this command to unconfigure transport-type.

Command Syntax

```
transport (ipv4|ipv6)
no transport
```

Parameters

Ipv4	IPv4 Transport Type
Ipv6	IPv6 Transport Type

Command Mode

PTP CLock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#transport ipv6
```

ttl

Use this command to set ttl value. Applicable for g.8275.2 profile.

Use no form of this command to set default value 64.

Command Syntax

```
ttl VALUE
no ttl
```

Parameters

<1-255>	Setting ttl value (default is 64)

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#ttl 2
```

unicast-grant-duration

Use this command to set unicast-grant-duration value. Applicable for g.8275.2 profile. Default is 300.

Use no form of this command to set default value 300.

Command Syntax

```
unicast-grant-duration <60-1000>
no unicast-grant-duration
```

Parameters

<60-1000>	Unicast-grant-duration value (default is 300)

Command Mode

PTP Clock Port mode

Applicability

This command introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#ptp clock profile g8275.2
(config-ptp-clk)#clock-port 1
(config-clk-port)#unicast-grant-duration 70
```

SECTION 13 Synchronous Ethernet

Synchronous Ethernet Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Configuring Synchronous Ethernet

This chapter shows how to configure Synchronous Ethernet. This chapter shows two scenarios in selecting a frequency source:

- Using quality level
- Using priority

Topology

In the topology shown in Figure 1-117, SW2 can select a clock source from SW1 or SW3. The selection is based on quality level or priority.

Note: We can enable SyncE on the physical interfaces which can be L2, L# or member port of the LAG.

Figure 1-117: Selecting a Frequency Source

Using Quality Level

In the procedure below, SW1 and SW3 are both configured as output sources, with SW1 having quality level QL_PRC and SW3 having quality level QL_SSU_A. SW2 is configured to accept a frequency from either SW1 or SW3. Because quality level is used as the clock selection criteria (the default setting), SW2 chooses SW1 as the frequency source.

SW1

`#configure terminal`	Enter configure mode.
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit configure Synchronous Ethernet mode.
`(config)#interface eth6`	Configure interface eth6.
`(config-if)#switchport`	Configure eth6 as a layer 2 port.
`(config-if)# bridge group 1`	Configure the interface to be part of bridge 1.
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#output-source`	Configure the interface as an output source.
`(config-if-synce)#quality-level QL_PRC`	Assign the quality level as PRC.
`(config-if-synce)#exit`	Exit interface Synchronous Ethernet mode.
`(config-if)#exit`	Exit interface mode.

SW2

`(config)#interface eth9`	Configure interface eth9.
`(config-if)#switchport`	Configure eth9 as a layer 2 port.
`(config-if)# bridge group 1`	Configure the interface to be part of bridge 1.
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#input-source 2`	Configure the interface as an input source with priority 2.
`(config-if-synce)#exit`	Exit interface Synchronous Ethernet mode.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth10`	Configure interface eth10.
`(config-if)#switchport`	Configure eth10 as a layer 2 port.
`(config-if)# bridge group 1`	Configure the interface to be part of bridge 1.
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#input-source 2`	Configure the interface as an input source with priority 2.
`(config-if-synce)#exit`	Exit interface Synchronous Ethernet mode.
`(config-if)#exit`	Exit interface mode.

SW3

`(config)#interface eth6`	Configure interface eth6.
`(config-if)#switchport`	Configure eth1 as a layer 2 port.
`(config-if)# bridge group 1`	Configure the interface to be part of bridge 1.
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#output-source`	Configure the interface as an output source.
`(config-if-synce)#quality-level QL_SSU_A`	Assign the quality level as SSU_A.
`(config-if-synce)#exit`	Exit interface Synchronous Ethernet mode.
`(config-if)#exit`	Exit interface mode.

Validation

SW1

1. Verify the Synchronous Ethernet details.

```
#Verify the output source.
#show synce output-sources
Interface Name  : eth6
Link State      : Up
QL Configured   : QL_PRC
QL Operational  : QL_PRC
```

SW2

1. Verify the input source.

```
#
Interface Name          : eth9
ESMC Status             : OK
Is-selected-Source      : Yes
QL Configured           : N/A
QL received in ESMC     : QL_PRC
QL Operational          : QL_PRC
Priority                : 2
Hold-off(ms)            : 300
Wait-to-restore(mins)   : 5
Link State              : Up
Signal Fail             : No
External Commands       : None
Clock-source-ID         : 256
WTR Timer Running       : No
Hold-off Timer Running  : No


Interface Name          : eth10
ESMC Status             : OK
Is-selected-Source      : No
QL Configured           : N/A
QL received in ESMC     : Ql_SSU_A
QL Operational          : Ql_SSU_A
Priority                : 2
Hold-off(ms)            : 300
Wait-to-restore(mins)   : 5
Link State              : Up
Signal Fail             : No
External Commands       : None
Clock-source-ID         : 256
WTR Timer Running       : No
Hold-off Timer Running  : No
```

2. Verify the Synchronous Ethernet details.

```
#
# show synce de
Equipment Clock         : EEC-option1
Interface Name          : eth9
ESMC Status             : OK
Is-selected-Source      : YES
QL                      : QL_PRC
SyncE Clock State       : Locked
DPLL Clock State        : Locked
Synce State Duration    : 00:02:25
Selected-Clk-Src-ID     : 256
```

SW3

1. Verify the Synchronous Ethernet details.

```
#
#show synce de
```

```
Equipment Clock          : EEC-option1
SyncE Clock State        : Free-run
DPLL Clock State         : Free-run
```

2. Verify the output source on SW3.

```
#
Interface Name  : eth6
Link State      : Up
QL Configured   : QL_SSU_A
QL Operational  : QL_SSU_A
```

Note: Use "`show synce stats`" to check the counter statistics and use "`clear synce stats`" to clear the counters. Show esmc counters changed to show synce stats.

Using Priority

In the procedure below, SW1 and SW3 in Figure 1-117 are both configured as output sources, with SW1 having priority 2 and SW3 having priority 1. SW2 is configured to accept a frequency from either SW1 or SW3. Because quality level is not used as the clock selection criteria (an explicit setting), SW2 chooses SW3 (with the higher priority) as the frequency source.

SW1

`#configure terminal`	Enter configure mode.
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#clock-selection mode ql-disabled`	Disable quality level checking.
`(config-synce)#exit`	Exit configure Synchronous Ethernet mode.
`(config)#interface eth6`	Configure interface eth6.
`(config-if)#switchport`	Configure eth6 as a layer 2 port.
`(config-if)#bridge group 1`	Configure the interface to be part of bridge 1
`(config-if)#synce`	Enter interface Synchronous Ethernet mode.
`(config-if-synce)#mode synchronous`	Configure synchronous mode.
`(config-if-synce)#output-source`	Configure the interface as an output source.
`(config-if-synce)#quality-level QL_PRC`	Assign quality level as PRC.
`(config-if-synce)#exit`	Exit interface Synchronous Ethernet mode.
`(config-if)#exit`	Exit interface mode.

SW2

`#configure terminal`	Enter configure mode.
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#clock-selection mode ql-disabled`	Disable quality level checking.
`(config-synce)#exit`	Exit configure Synchronous Ethernet mode

(config)#interface eth9	Configure interface eth9.
(config-if)#switchport	Configure eth9 as a layer 2 port.
(config-if)#bridge group 1	Configure the interface to be part of bridge 1
(config-if)#synce	Enter interface Synchronous Ethernet mode.
(config-if-synce)#mode synchronous	Configure synchronous mode.
(config-if-synce)#input-source 2	Configure the interface as an input source with priority 2.
(config-if-synce)#exit	Exit interface Synchronous Ethernet mode.
(config-if)#exit	Exit interface mode.
(config)#interface eth10	Configure interface eth10.
(config-if)#switchport	Configure eth10 as a layer 2 port
(config-if)#bridge group 1	Configure the interface to be part of bridge 1
(config-if)#synce	Enter interface Synchronous Ethernet mode.
(config-if-synce)#mode synchronous	Configure synchronous mode.
(config-if-synce)#input-source 1	Configure the interface as an input source with priority 1.
(config-if-synce)#exit	Exit interface Synchronous Ethernet mode.
(config-if)#exit	Exit interface mode.

SW3

#configure terminal	Enter configure mode.
(config)#synce	Enter configure Synchronous Ethernet mode.
(config-synce)#synchronization option 1	Configure synchronization network as option 1.
(config-synce)#clock-selection mode ql-disabled	Disable quality level checking.
(config-synce)#exit	Exit configure Synchronous Ethernet mode.
(config)#interface eth6	Configure interface eth6.
(config-if)#switchport	Configure eth6 as a layer 2 port.
(config-if)#bridge group 1	Configure the interface to be part of bridge 1
(config-if)#synce	Enter interface Synchronous Ethernet mode.
(config-if-synce)#mode synchronous	Configure synchronous mode.
(config-if-synce)#output-source	Configure the interface as an output source.
(config-if-synce)#quality-level QL_SSU_A	Assign quality level as SSU_A.
(config-if-synce)#exit	Exit interface Synchronous Ethernet mode.
(config-if)#exit	Exit interface mode.

Validation

SW1

1. Verify the Synchronous Ethernet details.

```
#show synce de
Equipment Clock         : EEC-option1
SyncE Clock State       : Free-run
```

```
DPLL Clock State        : Free-run
Synce State Duration    : 00:39:20
```

2. Verify the output source.

```
#show synce output-sources
Interface Name  : eth6
Link State      : Up
QL Configured   : QL_PRC
QL Operational  : QL_PRC
```

SW2

1. Verify the input source.

```
Interface Name          : eth9
ESMC Status             : OK
Is-selected-Source      : No
QL Configured           : N/A
QL received in ESMC     : QL_PRC
QL Operational          : QL_PRC
Priority                : 2
Hold-off(ms)            : 300
Wait-to-restore(mins)   : 5
Link State              : Up
Signal Fail             : No
External Commands       : None
Clock-source-ID         : 256
WTR Timer Running       : No
Hold-off Timer Running  : No


Interface Name          : eth10
ESMC Status             : OK
Is-selected-Source      : Yes
QL Configured           : N/A
QL received in ESMC     : Ql_SSU_A
QL Operational          : Ql_SSU_A
Priority                : 2
Hold-off(ms)            : 300
Wait-to-restore(mins)   : 5
Link State              : Up
Signal Fail             : No
External Commands       : None
Clock-source-ID         : 256
WTR Timer Running       : No
Hold-off Timer Running  : No
```

2. Verify the Synchronous Ethernet details.

```
# show synce de
Equipment Clock         : EEC-option1
Interface Name          : eth10
ESMC Status             : OK
Is-selected-Source      : YES
QL                      : QL_SSU_A
SyncE Clock State       : Locked
DPLL Clock State        : Locked
```



```
Synce State Duration    : 00:02:25
Selected-Clk-Src-ID     : 256
```

SW3

1. Verify the Synchronous Ethernet details.

```
#show synce de
Equipment Clock         : EEC-option1
SyncE Clock State       : Free-run
DPLL Clock State        : Free-run
Synce State Duration    : 00:39:20
```

2. Verify the output source.

```
#show synce output-sources
Interface Name  : eth6
Link State      : Up
QL Configured   : QL_SSU_A
QL Operational  : QL_SSU_A
```

Synchronous Ethernet Command Reference

Contents

This document contains these chapters:

CHAPTER 1 SyncE Commands

This chapter describes the Synchronous Ethernet configuration commands:

clock-selection mode

Use this command to set whether to use the Quality Level (QL) as a criteria when selecting a clock.

Use the no form of this command to set the QL to its default (`ql-enabled`).

Command Syntax

```
clock-selection mode (ql-enabled|ql-disabled)
no clock-selection
```

Parameters

`ql-enabled`	Use the quality level as a criteria when selecting a clock
`ql-disabled`	Do not use the quality level as a criteria when selecting a clock

Default

The default value is `ql-enabled`.

Command Mode

Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#synce
(config-synce)#clock-selection mode ql-enabled

(config-synce)#no clock-selection
```

clock-source-id

Use this command to set the clock source ID for Synchronous Ethernet interface.

Use the no form of this command to unset this value.

Note: Assign the same clock source ID if interfaces are connected to same clock source.

Command Syntax

```
clock-source-id <1-255>
no clock-source-id
```

Parameters

<1-255>	Clock Source ID.

Command Mode

Interface Synchronous Ethernet Mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#synce
(config-if-synce)#clock-source-id 1
```

dpll3-select

Use this command to select dpll3 as fixed input 10MHZ-IN.

Use no form of this command to unset this configuration.

Command syntax

```
dpll3-select 10mhz-in
no dpll3-select
```

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#dpll3-select 10mhz-in
```

hold-off

Use this command to set the hold-off time in milliseconds. The hold-off time ensures that short activation of signal fail is not passed to the selection process.

Use the no form of this command to set the default value (300 milliseconds).

Command syntax

```
hold-off <300-1800>
no hold-off
```

Parameters

<300-1800>	Hold-off time in milliseconds

Default

The default value is 300 milliseconds.

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#hold-off 500

(config-if-synce)#no hold-off
```

holdover

Use this command to set Synchronous holdover. Applicable only for 10MHz out interface.

Use no form of this command to disable holdover.

Command Syntax

```
holdover (<0-1440>|)
no holdover
```

Parameters

<0-1440>	Synchronous holdover range in minutes.

Command Mode

Synchronous Ethernet Mode

Default

Default Synchronous holdover is 10 minutes.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#synce
(config-synce)#holdover 2
```

input-source

Use this command to set an input timing source. Synchronization packets are received from this source and sent to the clock selection algorithm.

Use the no form of this command to delete an input source.

Command Syntax

```
input-source <0-255>
no input-source
```

Parameters

<0-255>	Priority: 1 is the highest, 255 is the lowest; 0 means the source will not be considered by the clock selection algorithm

Default

The default value is 0 meaning the interface will not be considered by the clock selection algorithm.

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#input-source 1
```

mode

Use this command to configure the interface as synchronous or non-synchronous:

- Synchronous interfaces extract the frequency of their input signal from synchronization packets and passes them to their internal clocks.
- Non-synchronous interfaces do not participate in the synchronization process.

Use the no form of this command to set the mode to its default (`non-synchronous`).

Command Syntax

```
mode (synchronous | non-synchronous)
no mode
```

Parameters

`synchronous` Synchronous mode

`non-synchronous` Non-synchronous mode

Default

The default value is `non-synchronous`.

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#mode synchronous

(config-if-synce)#no mode
```

output-source

Use this command to use an Ethernet interface as a timing output source.

Use the no form of this command to stop using an Ethernet interface as a timing output source.

Command Syntax

```
output-source
no output-source
```

Parameters

None

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#output-source
```

quality-level

Use this command to set the quality level (QL) for the timing source.

Use the no form of this command unconfigure quality-level on a port.

Command Syntax

```
quality-level QL_VAL
no quality-level
```

Parameters

QL_VAL	Quality level. The quality level you can specify depends on setting of the synce-interface command. See ITU-T Rec. G.781 for details.
QL_PRC	Primary Reference Clock
QL_SSU_A	Types I or V slave clock
QL_SSU_B	Type VI slave clock
QL_SEC	SDH Equipment Clock
QL_DNU	Do not use this signal for synchronization
QL_STU	Synchronized – traceability unknown
QL_ST2	Traceable to stratum 2
QL_ST3E	Traceable to stratum 3E
QL_SMC	Traceable to SONET clock self timed
QL_PROV	Provisionable by the network operator

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#quality-level QL_PRC
```

sync (configure mode)

Use this command to configure Synchronous Ethernet.

This command changes the mode from configure mode to configure Synchronous Ethernet mode and initializes the global Synchronous Ethernet parameters.

Use no form of this command to disable synce.

Command Syntax

```
synce
no synce
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#synce
(config-synce)
```

synce (interface mode)

Use this command to enable Synchronous Ethernet for an interface.

This command changes the mode from interface mode to interface Synchronous Ethernet mode.

This command does not automatically start synchronization distribution. You must explicitly give the mode command, specifying the `synchronous` option.

Use the `no` form of this command disable Synchronous Ethernet for an interface.

Command Syntax

```
synce
no synce
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#
```

synce debug

Use this command to turn on debugging.

Use the no from of this command to turn off debugging

Command Syntax

```
synce debug (event|recvd|trans)
no synce debug (event|recvd|trans)
```

Parameters

`event`	Enable event debugging
`recvd`	Enable reception debugging
`trans`	Enable transmission debugging

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#synce debug event
```

synce-interface

Use this command to enable Synchronous Ethernet for both GPS and 10MHz interfaces as input interfaces. This command changes the mode from interface mode to Synchronous interface Ethernet mode.

Use no form of this command to delete synce interface.

Command Syntax

```
synce-interface (gps | 10mhz-in|ptp)
no synce-interface (gps | 10mhz-in|ptp)
```

Parameters

`gps`	Input interface as GPS
`10mhz-in`	Input interface as 10MHz
`ptp`	PTP interface as input-source

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
(config)#interface eth1
(config-if)#synce-interface gps
(config-synce-if)#
```

synchronization option

Use this command to set the synchronization option for the internal clock that is locked in frequency to an incoming signal.

Use the no form of this command to set the default synchronization option (1).

Command Syntax

```
synchronization option (1 | 2)
no synchronization option
```

Parameters

1	Networks optimized for the 2048 kbit/s hierarchy
2	Networks optimized for the 1544 kbit/s hierarchy that includes the rates 1544 kbit/s, 6312 kbit/s, and 44 736 kbit/s

Default

The default value is 1.

Command Mode

Configure Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#synce
(config-synce)#synchronization option 2

(config-synce)#no synchronization option
```

wait-to-restore

Use this command to set the wait-to-restore timer in minutes. The wait-to-restore time ensures that a synchronization source that previously failed is considered by the selection process again only if it is fault free for a certain time.

Use the no form of this command to set the default wait-to-restore time (5 minutes).

Command syntax

```
wait-to-restore <0-12>
no wait-to-restore
```

Parameters

<0-12>	Wait-to-restore time in minutes

Default

The default value is 5 minutes.

Command Mode

Interface Synchronous Ethernet mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth1
(config-if)#synce
(config-if-synce)#wait-to-restore 1

(config-if-synce)#no wait-to-restore
```

CHAPTER 2 SyncE Show Commands

This chapter describes the Synchronous Ethernet show commands:

show synce stats

Use this command to display Ethernet Synchronization statistics.

Note: Show esmc counters changed to show synce stats.

Command Syntax

```
show synce stats
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show synce stats
Interface Name    Status      ESMC Received  ESMC Sent
_____________________________________________________
xe47                OK          1_________________1
xe48                OK          5_________________2
```

show synce details

Use this command to display details of the clock most recently selected by the Clock Selection Algorithm (CSA).

Command Syntax

```
show synce details
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show synce details
Equipment Clock         : EEC-option1
Interface Name          : eth9
ESMC Status             : OK
Is-selected-Source      : YES
QL                      : QL_PRC
SyncE Clock State       : Locked
DPLL Clock State        : Locked
Synce State Duration    : 00:03:26
Selected-Clk-Src-ID     : 256
```

show synce input-sources

Use this command to display details of all interfaces that are configured as Synchronous Ethernet input sources.

Command Syntax

```
show synce input-sources
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show synce input-sources
Interface Name          : xe1
ESMC Status             : OK
Is-selected-Source      : YES
QL Configured           : QL_PRC
QL received in ESMC     : QL_PRC
Operational QL          : QL_PRC
Priority                : 1
Hold-off(ms)            : 300
Wait-to-restore(mins)   : 5
Signal Fail             : No
External Commands       : None
Clock-source-ID         : 256
WTR Timer Running       : No
Hold-off Timer Running  : No
```

show sync output-sources

Use this command to display details of all interfaces that are configured as Synchronous Ethernet output sources.

Command Syntax

```
show synce output-sources
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show synce output-sources
Interface Name  : eth6
Link State      : Up
QL Configured   : QL_PRC
QL Operational  : QL_DNU
```

SECTION 14 sFlow

Sampling Flow Configuration Guide

Contents

This document contains this chapter:

CHAPTER 1 sFlow Configuration

This chapter provides the steps for configuring Sampled Flow (sFlow).

sFlow is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

The sFlow agent samples packets as well as polling traffic statistics for the device it is monitoring. The packet sampling is performed by the switching/routing device at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs as well as sampled packets to an sFlow collector for analysis.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

The sFlow agent uses the following forms of sampling:

- Sampling packets: samples one packet out of a defined sampling rate. This sampling is done by hardware at wire speed.
- Sampling counters: polls interface statistics such as generic and Ethernet counters at a defined interval.

You must enable the sFlow feature and collector before enabling sFlow sampling on an interface.

You cannot globally enable sFlow sampling monitoring on all interfaces with a single command. Instead you must enable sFlow sampling on the required interfaces individually.

sFlow feature is supported on physical interface as well as LAG interface. Configuring sampling on a LAG interface will enable the same on all member ports part of that LAG interface.

Topology

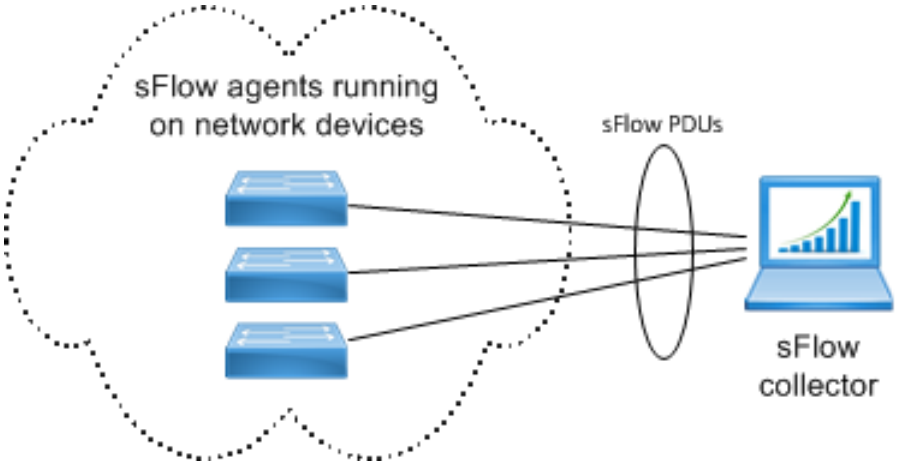


Figure 1-118: Basic sFlow topology

Configuration

sFlow Agent

`#configure terminal`	Enter configure mode.
`(config)#feature sflow`	Enable the sFlow feature.

(config)#sflow collector 2.2.2.2 port 6343 receiver-time-out 0 max-datagram-size 200	Configure the sFlow collector
(config)#interface xe1	Enter interface mode
(config-if)#sflow poll-interval 5	Set the counter poll Interval on the interface.
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200	Set the sFlow sampling interval on the interface in ingress directions.
(config-if)#sflow sampling-rate 1024 direction egress max-header-size 120	Set the sFlow sampling interval on the interface in egress directions.
(config-if)#sflow enable	Start packet sampling on the interface
(config-if)#end	Exit interface and configure mode.

Validation

```
#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.132
Collector IP: 10.156.159.29    Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-
Polling         Maximum Header
                  Rate                    Count               Interval
Count        Size(bytes)
         Ingress     Egress      Ingress     Egress      (sec)
Ingress     Egress
---------  ----------------------   ----------------------  ----------------
-------   --------------------
xe1/1           1024        1024       464564        414532          5
131     120          20
```

Sampling Flow Command Reference

Contents

This document contains this chapter:

CHAPTER 1 sFlow Commands

This chapter describes the Sampled Flow (sFlow) commands.

clear sflow statistics

Use this command to clear sFlow sampling-related counters such as the number of packets sampled and the number of counters sampled.

Command Syntax

```
clear sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear sflow statistics
```

debug sflow

Use this command to display sFlow debugging messages.

Command Syntax

```
debug sflow (all|agent|sampling|polling|)
```

Parameters

`all`	Debug all (agent,sampling,polling)
`agent`	Debug sFlow agent
`sampling`	Debug sFlow sampling
`polling`	Debug sFlow polling

Default

By default, debug command is disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug sflow all
#debug sflow agent

#configure terminal
(config)#debug sflow agent
```

feature sflow

Use this command to enable the sFlow feature.

Use the no form to disable the sFlow feature.

Command Syntax

```
feature sflow
no feature sflow
```

Parameters

None

Default

By default, sFlow feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#feature sflow
```

sflow agent-ip

Use this command to set the agent IP address for receivers.

Use the no form of this or remove an agent IP address.

Command Syntax

```
sflow agent-ip A.B.C.D
no sflow agent-ip
```

Parameter

A.B.C.D	IPv4 address

Default

The default IP address is zero (0).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#sflow agent-ip 10.0.0.12
```

sflow collector

Use this command to configure the collector details such as the collector IPv4 address, port number, receiver time-out and datagram size.

Use the no form of this command to disable the sFlow collector.

Command Syntax

```
sflow collector A.B.C.D port <1024-65535> receiver-time-out <0-2147483647>
  max-datagram-size <200-9000>
no sflow collector (A.B.C.D port <1024-65535> receiver-time-out <0-2147483647> max-
  datagram-size <200-9000> |)
```

Parameter

A.B.C.D	Collector IPv4 address
<1024-65535>	Collector UDP Port number. The standard sFlow UDP Port : 6343
<0-2147483647>	Receiver time out value in seconds. Zero means no timeout. Upon timeout, value collector information is removed, stopping any ongoing sampling.
<200-9000>	Maximum datagram size in bytes that can be sent Collector

Default

By default, sFlow collector is disabled. Default port number is 6343.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#sflow collector 2.2.2.2 port 1111 receiver time-out 30 max-datagram-
size 500

(config)#no sflow collector
```

sflow enable

Use this command to enable or disable sampling on an interface after giving the sflow sampling-rate command on the same interface.

Command Syntax

```
sflow enable
no sflow enable
```

Default

By default, sFlow sampling is disabled.

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-datagram-size 200
(config-if)#sflow enable
(config-if)#no sflow enable
```

sflow poll-interval

Use this command to configure the sFlow counter polling interval. Any change in the polling interval restarts ongoing polling of existing data source interfaces, if any.

Use the no form of this command to disable the sFlow counter polling interval.

Command Syntax

```
sflow poll-interval <5-60>
no sflow poll-interval <5-60>
```

Parameters

<5-60>	Interface counter. Polling interval in seconds

Default

By default, sFlow counter polling interval is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow poll-interval 25
(config-if)#no sflow poll-interval 25
```

sflow rate-limit

Use this command to set the CPU rate limit in packets per second.

Use the no form of this command to set the CPU rate limit to its default (0).

Command Syntax

```
sflow rate-limit <2000-100000>
no sflow rate-limit
```

Parameters

<2000-100000>	Rate limit in packets per second

Default

The default rate limit is zero (0).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Examples

```
#configure terminal
(config)#sflow rate-limit 5000
```

sflow sampling-rate

Use this command to set the sampling rate on an interface. Any change in the sampling rate restarts the ongoing sampling of existing data-source interfaces, if any.

Use the no form of this command to disable the sFlow sampling rate.

Note: Packets to CPU is rate limited. In case of unknown unicast, rate limit is applied to such packets as well as sampled data packets.

Command Syntax

```
sflow sampling-rate <1024-1073741823> direction (ingress | egress) max-header-size
  <128-256>
```

```
no sflow sampling-rate <1024-1073741823> direction (ingress | egress) max-header-
  size <128-256>
```

Parameters

`<1024-1073741823>`	
	Sampling rate
`direction`	The direction of sampling an interface:
`ingress`	Ingress traffic
`egress`	Egress traffic
`<128-256>`	Maximum header size in bytes

Default

By default, sFlow sampling rate is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200
(config-if)#no sflow sampling-rate 1024 direction ingress max-header-size 200
```

show sflow

Use this command to display sFlow agent configuration along with statistics for all interfaces.

Command Syntax

```
show sflow (brief | detail)
```

Parameters

`brief`	Display configuration parameters on interfaces along with sampling rate and poll interval.
`detail`	Same as `brief` along with configured and default attributes and values of sFlow agent, sFlow collector, and sampling information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show sflow
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.12.16.38
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-Polling         Maximum Header
                 Rate                     Count               Interval       Count        Size(bytes)
           Ingress      Egress       Ingress      Egress       (sec)                     Ingress     Egress
---------  ----------------------   ----------------------  ----------------------   -------------------
xe1            1024            0            0            0           6            3     128            0

#
#show sflow brief
sFlow Feature: Enabled
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Configuration:
Interface   Status               Sample Rate               Counter-Polling
            Ingress    Egress    Ingress      Egress       Interval(sec)
---------   ------------------   ----------------------   ---------------
xe1       Enabled    Disabled         1024            0      6
```

Table 1-72: Show sflow output

Entry	Description
sFlow feature	Shows whether sFlow is enabled or disabled.
sFlow Version	Displays the sFlow version. Version 5 is the current global standard.
sFlow Global Information	Global Information consists of the Agent IP address, Collector IP, Port number, Maximum Datagram Size, and the Receiver timeout.
Agent IP	IPv4 address of this switch/router.
Collector IP	IPv4 address of the sFlow collector server.
Port	Port number on the sFlow collector server. Standard is port 6343.
Maximum Datagram Size	The maximum size of the datagrams sent by the agent
Receiver timeout	The number of seconds between each sampling – zero means sample continuously.
sFlow Port Interface	The interface of this switch/router on which sFlow is running (e.g. xe1/1).
Packet-Sampling Rate	the number of packets received or transmitted before a sample is taken.
Packet-Sampling Count	The number of sample packets that have been sampled on both the ingress and egress of the interface.
Counter-Polling	Shows the amount of time between polling samples and the count of the total number of polling samples taken.
Maximum Header Size	The maximum header size for both the ingress and egress of the interface.

show sflow interface

Use this command to display the sFlow configuration for the input interface.

Command Syntax

```
show sflow interface IFNAME
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow interface xe1
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.104
Collector IP: 10.12.16.18      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Counter-Polling           Maximum Header
           Rate         Count        Interval(sec) Count       Size(bytes)
---------  -----------------------   ------------------------  --------------
xe1              1024            0           6           41      128
```

show sflow statistics

Use this command to display sFlow counter information.

Command Syntax

```
show sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow statistics

sFlow Port Statistics:
Interface  Packet-Sampling   Counter-Polling
                Count              Count
---------  ---------------   ---------------
xe1                     0                19
```

SECTION 15 Quality of Service

Quality of Service Configuration Guide

Contents

This document contains these chapters.

CHAPTER 1 Quality of Service (QoS)

This chapter contains a general overview of QoS functionality and terminology.

QoS Functionality

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

QoS is based on DiffServ architecture, which stipulates that individual packets be classified upon entry into a network. Classification information can be carried in the Layer-3 IP packet header or the Layer-2 frame. IP packet headers carry the information using 6-bits from the deprecated IP type of service (TOS) field. Layer-2 802.1Q frames carry the information using a 2-byte Tag Control Information field. All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

- End hosts or switches along a path, based on a configured policy
- Detailed packet examination, expected to occur nearer to the network edge, to prevent overloading core switches and routers
- A combination of the above two techniques

Class information can be used by switches and routers along a path to limit the amount of allotted resources per traffic class. Per-hop behaviour is an individual device’s behaviour when handling traffic in the DiffServ architecture. An end-to-end QoS solution can be created if all devices along a path have consistent per-hop behaviour.

Quality of Service (QoS) provides preferential treatment to specific traffic, possibly at the expense of other traffic. Without QoS, Qumran offers best-effort service to each packet, however, this may cause unpredictable network behaviour. Implementing QoS in a network makes performance more predictable and bandwidth utilization more effective.

QoS design in Qumran complies with IETF-DiffServ and IEEE 802.1p standards. A typical QoS model deployment is based on the following elements:

- The packet received on customer edge port will be assigned to a QoS service. The service is assigned based on the packet header information.
- The QoS service defines the packet's internal QoS handling (i.e. traffic class/queue and drop precedence/color) and optionally the packet's external QoS marking, through either the IEEE 802.1p User Priority or the IP header DSCP field.
- Qumran provides end-to-end QoS behavior by providing consistent QoS treatment to the traffic within the network core based on packet's IEEE 802.1 or DSCP marking.
- Qumran can modify the assigned service of the packets if a packet stream exceeds the ingress configured rate by marking drop precedence and remarking packet's IEEE 802.1p or DSCP at the egress.
- Qumran incorporates the required QoS features to implement network-edge, as well as, network-core devices.
- Qumran provides flexible mechanisms to classify packets into different service levels.
- Service application mechanism is based on eight egress priority queues per port.
- The packet Priority fields can be remarked to reflect the QoS assignment on L2 and L3 networks.

  Note: Packet priority remarking on an MPLS network is not supported.

Terminology

Following is a brief description of terms and concepts used to describe QoS.

ACL

Access control lists (ACLs) classify traffic with the same characteristics.

CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network. QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic.CoS values range from zero to seven, seven being the highest priority.

DSCP Value

DSCP Value Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network. DSCP values range from 0 to 63, 63 being the highest priority, 0 being best-effort traffic.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs. Classification occurs on an ingress physical port. Classification can be based on QoS ACLs, or class maps and policy maps.

Policing

Policing can occur on ingress interfaces. Policer limits the bandwidth consumed by a traffic flow with the results given to the marker. The two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration data to determine the action required for the packet, and then handles the packet using one of the following methods:

- Let the packet through without modification
- Drop the packet

Marking can occur on ingress and egress interfaces.

Queuing

Queuing maps packets to a queue. Each egress port can accommodate up 8 queues, prioritized as 0 lowest and 7 highest. The tagged packet incoming priority can be mapped to one of the 8 queues obtained from the filtering

mechanism result. The untagged packet priority is also obtained from the filtering mechanism result. After the packets are mapped to a queue, they are scheduled.

Scheduling

Scheduling forwards or conditions packets using one of the following methods:

- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted. Strict Priority will be operating on the remaining bandwith available for the Port
- WFQ (Weighted Fair Queuing) weight-based scheduling – In this scheduling, some weight based bandwidth is allocated to all queues. In this scheduling, egress traffic will be served based on the configured weight distribution.
- Combination of WFQ and SP, the Remaining Bandwidth will be scheduled in the strict order for the SP Queues. The Remaining Bandwidth will be scheduled in the WFQ mode for WFQ Queues.

Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to classify it further. The criteria can include:

- Matching the access group defined by the ACL
- Matching a specific list of CoS, DSCP, Exp and etc.

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

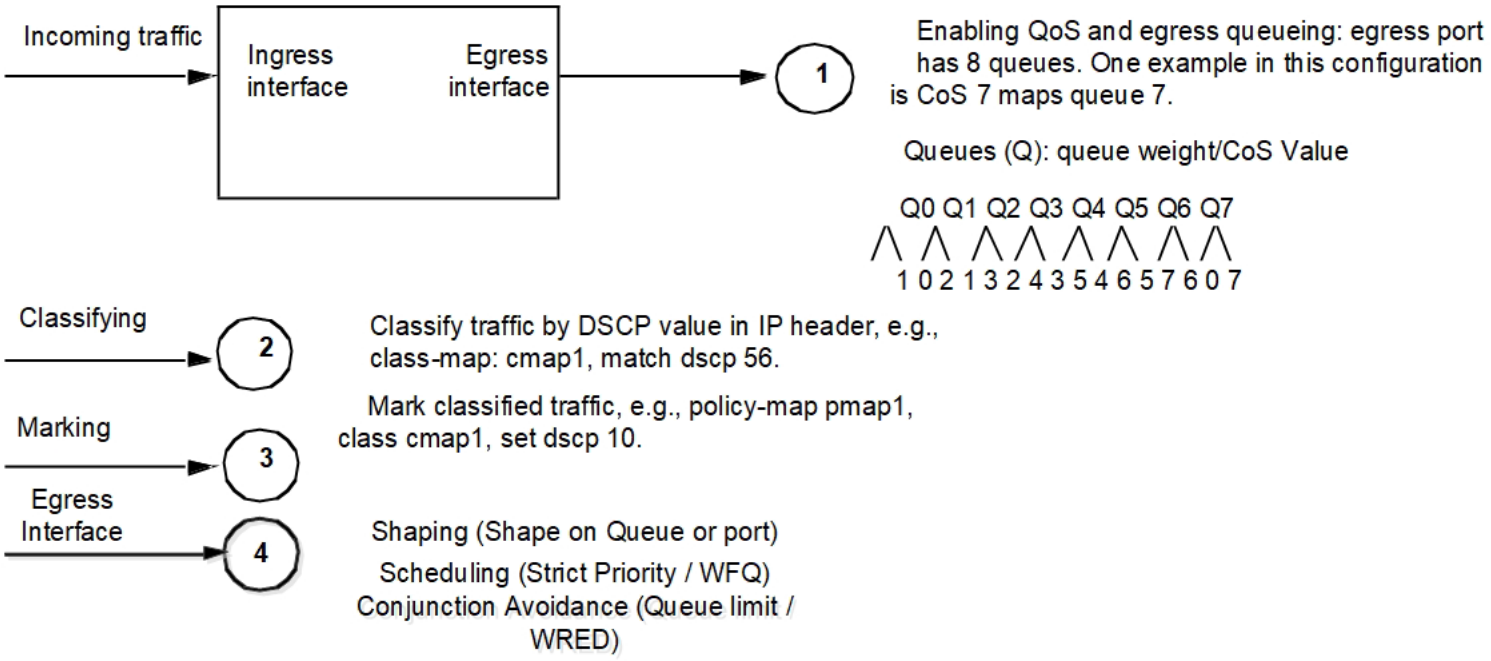
Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

- Set a specific CoS or DSCP value in the traffic class.
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.

Policy maps have the following attributes:

- A policy map can contain Maximum 256 class-map per policy-map, each with different match criteria and policers.
- A separate policy-map class can exist for each type of traffic received through an interface.
- There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.
- Before a policy map can be effective, it must be attached to an interface.



QoS model

This section explains the implementation and configuration details of QoS:

Traffic types

Data — Packets can be network-to-network traffic or traffic from CPU. Network-to-network packets are considered data traffic and QoS parameters can be applied on data traffic.

Control — Packets to and from the CPU are considered as control traffic. Incoming control traffic is prioritized based on ingress map and are sent to their own designated CPU queues. Each CPU queue has a fixed rate limit to guard the CPU. Outgoing control traffic will always be sent on highest priority queue (Q7) on the data port.

Setting packet header QoS fields

The device supports modifying the packets header IEEE 802.1p user priority or IP-DSCP.

Packet QoS Attributes

Every data packet is assigned a set of QoS attributes that can be modified in several stages of the ingress pipeline engine.

The ingress pipeline engine also contains a QoS Remark option for L3 traffic that can modify the initial QoS attributes of the packet.

Color and Drop Precedence relation: Green has the lowest drop precedence, Yellow has a higher drop precedence, and Red has the highest drop precedence. See Table 1-73.

Table 1-73: Packet QoS attributes

QoS Parameter	Description
TC (Traffic Class or queue)	This is the priority level assigned to the packet. When the transmission engine queries the packet, it uses this field to select the appropriate priority queue
DP (Drop Precedence or color)	The transmission engine uses this field for congestion resolution. Packets with higher drop precedence are more likely to be discarded in the event of congestion. By default, packets with red color will be dropped by a Qumran even if there is no congestion. Disabling red packet drop is configurable per device. In case of L2 packet, DEI 0 will be marked to color green and DEI 1 will be marked to color yellow. In case of L3 packet, AFx1 will be marked as green while both AFx2 and AFx3 will be marked as yellow (where x=1,2,3).

CHAPTER 2 Configuring a QoS Policy-map

The following section explains the configuration of basic infrastructure to apply QoS treatment on the ingress interface.

Ingress QoS treatment can be achieved by two types of configuration.

- Policy-map configuration
- Profile mapping configuration

This section explains policy-map configuration method. QoS feature must be enabled to configure policy-maps.

This infrastructure contains two entities - class-map and policy-map. Class-map holds the match criteria and class-maps can be bound to policy-map to configure QoS treatment for the matching traffic.

Creating a QoS class-map

A Class-map contains the matching criteria for the traffic. Class-maps with no match criteria will match all the data traffic.

Class-maps support the following match criteria: vlan, inner vlan, cos, inner cos, dscp, precedence, layer4 tcp/udp port, exp, Ether-type, or ACL.

Class-map can be of two types, match-any or match-all type. By default class-map is of match-all type. For match-all class-maps, only the traffic that qualifies all match criteria configured in class-map will take QoS action. For match-any class-maps, traffic qualifying any one of the configured match criteria will take QoS action.

Class-maps can be created once the QoS feature is enabled.

Use the following command to create a class-map:

```
class-map (type qos|) (match-any|match-all|) NAME
```

This command will create a class-map entity that can be configured with one or more match criteria.

Class-map can be of two types:

1. Empty class-map: Class-map with no matching criteria is called empty class. Empty class will classify all the traffic coming on the port on which the policy containing empty class will be applied.
2. Non-empty class-map: Class-map with matching criteria is called non-empty class. It will classify the traffic according to the given matching criteria.

User can always add/delete/modify the matching criteria of the class-map. User is not allowed to make a non-empty class as empty class if the class is attached to a policy-map. User has to remove the class from policy-map to modify the matching criteria. User is allowed to add matching criteria to an empty class attached to a policy-map.

Use the following commands to add match criteria:

```
match vlan WORD
match vlan inner WORD
match cos WORD
match cos inner WORD
match dscp [WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef]
match precedence [WORD | critical | flash | flashoverride | immediate | internet | network | priority | routine]
match mpls experimental topmost WORD
match ip rtp WORD
match ethertype WORD
match layer4 (tcp|udp|any) (source-port|destination-port) WORD
```

```
match access-group NAME
```

An example of creating a class-map with match VLAN configuration is shown below:

```
(config)#qos enable
(config)#class-map n1-class-10
(config-cmap-qos)#match vlan 10
(config-cmap-qos)#exit
```

Notice that data traffic with an outer VLAN value of 10 will be matched for QoS treatment.

Creating a QoS policy-map

Policy-maps can be configured with multiple class-maps with each class-map configured with policing or other supported actions.

Use the following command to create a policy-map:

```
policy-map (type qos|) NAME
```

This command will create a policy-map entity in which one or more class-map entities can be bound.

Binding a class-map to a policy-map

In order to apply QoS treatment to traffic that matches the criteria configured in a class-map, the class-map must be bound to the policy-map entity, then QoS treatment actions can be configured on that node.

Use the following command to bind a class-map to a policy-map:

```
class (type qos|) NAME
```

This command will create a class node for class-map unique to the policy-map. This class node can then be configured with QoS treatment actions.

There are two types of actions, `police` and set.

- Police actions can be used to control the rate of traffic flow and is explained in the next section.
- Set actions can be used to set internal priority or packet priority.

Use the following commands to add set actions:

```
set (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))
set cos <0-7>
set queue <0-7>
```

An example of creating a policy-map and binding a class-map to it with the `set` action is shown below:

```
(config)#policy-map n1-police-10
(config-pmap-qos)#class n1-class-10
(config-pmap-c-qos)#set cos 3
(config-pmap-c-qos)#exit
(config-pmap-qos)#exit
```

In case of multiple class-maps, implicit priority of class-maps will be decided based on the following the type of class-map as shown:

match-all > match-any > default class-map

If all class-maps are of type match-all, the class-map with the higher number match criteria will have higher priority. If the class-maps have the same number of match criteria, then the behavior can be unpredictable if traffic matches both class-map criteria. In such cases, class-maps can be explicitly prioritized using the priority command.

priority <1-1000>

An example of configuring priority per class-map is shown below:

```
(config)#policy-map p1
(config-pmap-qos)#class c1
(config-pmap-c-qos)#priority 2
```

A higher the value means higher priority, and user defined priority is always higher prioritized over implicit priority.

If the match criteria is ACL, different hardware resources will be used. Therefore, configuring match ACL class-map and other non-ACL match classes in a single policy is not allowed because if a policy-map with two class-maps (one with ACL match criteria and one with some other match criteria) are allowed (configured in different hardware resource groups), traffic matching both match criteria can take actions of both class-maps if the actions are not conflicting but since statistics are common and can be read once (hardware limitation), statistics will be displayed for one matching criteria only.

Assumptions and limitations

DSCP and precedence matches are mutually exclusive and can't be part of same class-map.

Each rule of an ACL is matched independently, so ACL matches are allowed to be configured only on match-any type class-map. If the configured matches on class-maps bound to and interface via policy-map are not mutually exclusive, there are chances of multiple class-maps matching a single stream of traffic. In this case, implicit priority of the class-map based on number of rules decides which class-map the traffic will hit. When implicit priority is the same for class-maps, their behavior will be random, and the user is expected to configure class priority in such a case.

Binding a QoS policy-map

Policy-map configuration is effective only when it is bound to a supported ingress interface. Use the following command to bind a policy-map to an interface:

```
service-policy type qos input NAME
```

Notice that `NAME` represents the name of the qos policy-map.

Note: A QoS TCAM group must be enabled before binding a policy-map to an interface. Refer to the "*hardware-profile filters (Qumran)*" and "*show hardware-profile filters show (Qumran)*" sections in the *Command Reference Guide* for more information about the hardware filter groups.

An example of binding a policy-map to an interface is shown below:

```
(config)#hardware-profile filter qos-ext enable
(config)#interface xe1
(config-if)#service-policy type qos input n1-police-10
(config-if)#exit
```

In this example, traffic with VLAN value 10 received on interface `xe1` is matched by `class-map` configuration, and traffic will be set with internal and packet priority (cos) 3 (as shown in the previous example).

Note: For an ACL match configuration, ingress-l2-ext/ingress-ipv4-ext/ingress-ipv6 TCAM group must be enabled based on ACL type.

When the class-map is configured with match ACL, only the `police` action is supported – `set` actions are not supported.

CHAPTER 3 Traffic Policing

Traffic policing can be achieved by using a policy-map based method. Policy-map based configurations allow the flexibility to police the traffic per-port and a set of other matching criteria:

- VLAN (outer vlan and inner vlan)
- CoS (outer cos and inner cos)
- DSCP
- Topmost EXP
- Ether-typ
- Precedence
- TCP or UDP port
- ACL

Note: Qumran supports rate limiting of ingress traffic. Rate limiting egress traffic is not supported.

Applying Traffic Policing Parameters Using a policy-map

Policy-map based traffic policing can be achieved by binding policy-map on the interface in ingress direction. A policy-map is associated with two sections. One is class-map which will have match criteria configured. Other is police configuration to apply traffic policing on the matching traffic on the policy-map bound port in ingress direction (see Chapter 2, *Configuring a QoS Policy-map*).

Traffic policing determines the rate of ingress traffic that is allowed per port (traffic that matches the configuration in the class-map).

Note: Qumran supports two types of policing:

- Single rate three color traffic rate limiting (RFC 2697).
- Two rate three color traffic rate limiting (RFC 4115).

Single rate or two rate operations are in compliance with the RFCs mentioned.

Note: Packets marked with color red are dropped by default in Qumran devices. This default behavior can be modified with global command to disable red packet drop. However, traffic policing and storm control will not work if red packet drop is disabled.

For more information about color, refer to the Packet QoS Attributes section.

Configuration Considerations

- Policy map based rate limiting is supported only for ingress traffic.
- Only one policy-map of same type can be bound on an interface.
- One policy-map can have up to 256 class-maps.
- CIR and EIR configuration should be in same format. Example, if one of them is configured in percentage, other also should be configured in percentage.
- Minimum configurable rate is 22 kilobits per second.
- Minimum burst size supported is 1 kilo bytes and maximum burst size supported in 4161 kilo bytes.

Configuring Traffic Policing

The following section shows how to configure policing on an interface. Refer to Chapter 2, *Configuring a QoS Policy-map* for configuring policy-maps.

Note: Policer action must be configured on the class node to achieve traffic policing for matching traffic.

Use the following command to configure a policer for Qumran MX:

```
police (colour-blind | colour-aware |) (cir) (<1-720000000> (kbps|mbps|gbps) | percent
<1-100>) ((eir (<1-720000000> (kbps|mbps|gbps) | percent <1-100>)|) ((bc) <1-4161>
(kbytes|mbytes|ms|us)|) ((be) <1-4161> (kbytes|mbytes|ms|us)|))
```

Use the following command to configure a policer for Qumran AX:

```
police (colour-blind | colour-aware |) (cir) (<1-500000000> (kbps|mbps|gbps) | percent
<1-100>) ((eir (<1-500000000> (kbps|mbps|gbps) | percent <1-100>)|) ((bc) <1-4161>
(kbytes|mbytes|ms|us)|) ((be) <1-4161> (kbytes|mbytes|ms|us)|))
```

- For Qumran MX, the configuable rate range is 22kbps to 720gbps.
- For Qumran AX, the configuable rate range is 22kbps to 500gbps.

An example of creating a policy-map and binding a class-map to it with police action is shown below:

```
(config)#qos enable
(config)#class-map n1-class-10
(config-cmap-qos)#match vlan 10
(config-cmap-qos)#exit
(config)#policy-map n1-police-10
(config-pmap-qos)#class n1-class-10
(config-pmap-c-qos)#police cir 10 mbps eir 20 mbps
(config-pmap-c-qos)#exit
(config-pmap-qos)#exit
(config)#hardware-profile filter qos-policer enable
(config)#interface xe1
(config-if)#service-policy type qos input n1-police-10
(config-if)#exit
```

In the following example, traffic with vlan ID 10 received on interface `xe1` will be policed to a total of 30 mbps with 10 mbps of traffic being marked green, and 20 mbps of traffic marked yellow, any remaining traffic will be dropped at ingress.

Example configuration for color aware police:

```
(config-pmap-c-qos)#police colour-aware cir 10 mbps eir 20 mbps
```

With this configuration, if traffic with vlan ID 10 (with CFI bit set) is received on interface `xe1` it is “policed” to a total of 20 mbps only because the traffic will be treated as yellow and will be subjected only to the EIR bucket.

Displaying Rate Limiting Policies

Use the following commands to verify the configuration and statistics.

- `show policy-map` – This command displays the configuration of policy map.
- `show policy-map interface INTERFACE-NAME` – This command displays the policy-map details on the interface along with statistics of how many packets and bytes matches and how many packets and bytes are dropped due to policer.
- `show policy-map statistics type qos` – This command displays the statistics of matched packets and bytes and dropped packets and bytes per class-map in table format.

Note: Packets dropped by the policer are counted in policy-map drops, as well as in queue red drops because the hardware doesn't support policer action to directly drop the packet. Packets that need to be dropped are marked red and are dropped at the queue.

Use the following command to obtain QoS statistics:

```
qos statistics
```

Use the following command to clear QoS statistics.

```
clear qos statistics
```

Drop counters verification

Drop counters with drop reason can be verified globally using the following command:

```
#show hardware-discard-counters
+---------------------------------+---------+------------+------------+
| Registers                                 | Core 0     | Core 1     |
+---------------------------------+---------+------------+------------+
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER        1596100
   Reason: DP_LEVEL_STATUS                    Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER        59807
   Reason: SRC_EQUAL_DEST_INT                 Y
```

CHAPTER 4 Rate Limiting BUM Traffic

To prevent the CPU from getting flooded with Broadcast, Unknown Unicast, and Multicast (BUM) traffic, rate limiting can be applied at the ingress interface. This configuration is called “storm control” and is independent of the QoS feature, and can be configured directly on the interface in the ingress direction.

Configuring per port rate limiting for BUM traffic

BUM rate limiting can be configured on the interface via following command:

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000> (kbps|mbps|gbps))
```

The `broadcast` option is for broadcast traffic, `multicast` option is for multicast traffic and `dlf` (Destination Lookup Failure) option is for unknown unicast traffic.

There are two ways to configure the rate limiting information. One is in percentage and the other is in absolute values. Use the level option to configure in percentage format where the link speed is used for rate calculation. Percentage value can be configured with up to four fractional digits in order to support kbps level rate limiting on 100 gbps ports, and the Absolute configuration option uses the input rate in kbps, mbps, or gbps.

An example of BUM rate limiting is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#storm-control dlf 2 mbps
(config-if)#exit
```

In the configuration above, unknown unicast traffic received on `xe1` will be rate limited to 2 mbps.

Note: Packets marked with color red are dropped by default by Qumran devices. This default behavior can be modified with global command to disable red packet drop. However, traffic policing and storm control will not work if red packet drop is disabled

Displaying BUM rate limit information

Use the following command to verify BUM rate limit configuration:

```
show storm-control (INTERFACE-NAME|)
```

Note: Drop statistics for BUM rate limiting is not supported on Qumran.

CHAPTER 5 Ingress Traffic Processing

Qumran can process packets based on the priority information of the packet. During the packet processing, there are several opportunities to influence the processing by the following configurations:

1. Derive internal priority and drop precedence from the packets IEEE 802.1p (PCP) value and drop eligibility indicator (DEI) value. The Priority Code Point (PCP) is a 3-bit field within an 802.1Q tagged frame that is used to convey the internal priority of the frame and DEI is a single bit that is used to convey the drop precedence of the frame.

   Note: The PCP field was formerly called 802.1p.

2. Derive internal priority and drop precedence from the packets DSCP value.
3. Force modification of internal priority and drop precedence using user defined ingress mapping profile.
4. Force the internal priority value based on classification configured using policy maps. This is used for setting a specific priority for L2, L3 or L4 traffic flow.
5. Packet priority and drop precedence will be based on PCP and DEI values for the traffic received on switch ports. Similarly, packet priority and drop precedence will be based on DSCP value for the IPv4 traffic received router ports. For MPLS traffic on label switched interface, packet priority is based on topmost label's EXP value.
6. When trust level on switch ports is modified to trust DSCP values, packet priority and drop precedence for IPv4 traffic will be based on DSCP value.
7. Assign internal priority to untagged traffic on switch port with port level untagged priority configuration.

Mapping Inbound Packet Priorities to Internal Priorities

Priority and drop precedence information is collected from various portions of the packet header:

- If a tagged packet is received on a switch port, derive a priority value from PCP and drop precedence DEI value.
- If a tagged packet is received on a switch port on which trust level is set to DSCP, derive the priority value from DSCP bits. Drop precedence will be derived from DEI bit value.
- If an untagged packet is received on a switch port, assign priority value based on port level untagged priority configuration.
- If an untagged packet is received on a switch port on which trust level is set to DSCP, derive the drop precedence value from DSCP bits.
- If IPv4 packet is received on a router port, derive a priority value and drop precedence by decoding the DSCP bits.
- If MPLS packet is received on a label switched port, derive a priority value and drop precedence by decoding EXP bits.
- The derived values for PCP and DSCP are mapped to a default map.

CHAPTER 6 Modifying Internal Priority at Ingress

After the packet priority is recognized as PCP, DSCP or EXP values, priority queue and drop precedence will be determined by one of the following methods:

- Default ingress decode mappings are configured as explained in "Chapter 9, *Default QoS Mappings*."
- Global ingress mapping profiles are available for modification to configure non-default values on a Qumran device as explained in "Chapter 10, *Configuring QoS*". Following are the global ingress profiles affecting priority queues and drop precedence configuration:

  `qos profile cos-to-queue default` – Configuration in this profile allows modifying default mapping of PCP to priority queue globally.

  `qos profile dscp-to-queue default` – Configuration in this profile allows modifying default mapping of DSCP to priority queue and drop precedence globally.

  `qos profile exp-to-queue default` – Configuration in this profile allows modifying default mapping of EXP to priority queue and drop precedence globally.
- User-defined ingress decode mapping profiles can be created and bound to port to override the global configuration:

  `qos profile cos-to-queue NAME` – Configuration in this profile allows creating user-defined mapping of PCP to priority queue and can be bound to port to take effect.

  `qos profile dscp-to-queue NAME` – Configuration in this profile allows creating user-defined mapping of DSCP to priority queue and drop precedence and can be bound to port to affect.
- User-defined PCP to TC profile map can be bound to VPLS instance or per-VLAN-based attachment circuit and this mapping will override the profiles mapping bound to port or the global mapping profile.
- User-defined PCP to TC profile map can be bound to VPWS VLAN based attachment circuits and this mapping will override the profile mapping bound to port or the global mapping profile.
- User-defined PCP to TC profile map can be bound to registration entries for provider edge ports and this mapping will override the profile mapping bound to port or the global mapping profile.
- QoS policy-maps can be configured as explained in "Chapter 2, *Configuring a QoS Policy-map*" with set queue action and bound to an ingress port will override the priority queue configuration for the traffic that matches the policy-map configuration. Policy-map configured with `policer` action resulting in color marking will override the drop precedence on the traffic as per configuration.
- Internal priority for untagged traffic received on switch ports will be set to zero by default.
- Untagged traffic can be assigned with a non-default priority queue with port level configuration: `qos untagged-priority <0-7>` – This configuration assigns priority queue for untagged traffic received on the configured switch port.

CHAPTER 7 Remarking Packet Priority at Ingress

Apart from altering the internal priority and drop precedence, Qumran device allows modification of packet priority for PCP and DSCP values by one of the following methods:

- Configuration of ingress dscp-to-queue mapping profile allows the modification of DSCP value of the packet. This mapping is applicable only to IPv4 traffic on router port.
- QoS policy-maps can be configured with set CoS and set DSCP actions which will modify PCP or DSCP value of the packet, respectively. Set CoS action is applicable on switch ports and tagged packets. Set DSCP action is applicable on router port where IPv4 traffic is received on the port. Remarking DSCP through policy-map configuration will override the mapping profile remarking.

Note: Qumran does not support encoding EXP value from packet priority of tagged (PCP) or IPv4 traffic (DSCP) through ingress processing. EXP value encoding is supported only through egress processing.

Note: Refer Chapter 10, *Configuring QoS* for Remarking configuration.

CHAPTER 8 Remarking Packet Priority at Egress

In Qumran, tagged traffic PCP value on switch port and IPv4 traffic DSCP value on router port can be remarked through egress processing. When either the remark CoS or remark DSCP command is enabled on the egress port, one of the following remarkings takes place:

- Default egress encode mappings are configured as explained in “Chapter 9, *Default QoS Mappings*".
- Global egress mapping profiles are available for modification to configure non-default values on a Qumran device as explained in “Chapter 10, *Configuring QoS*”. Following are the global egress profiles affecting packet priority on traffic at egress:

  `qos profile queue-color-to-cos default` — Configuration in this profile allows modifying default mapping of internal priority and drop precedence to packet priority (PCP) globally.

  `qos profile dscp-to-dscp default` — Configuration in this profile allows modifying default mapping of DSCP and drop precedence to packet priority (DSCP) globally.

- User-defined egress encode mapping profiles can be created and bound to egress port to override the global configuration:

  `qos profile queue-color-to-cos NAME` — Configuration in this profile allows creating user-defined mapping of internal priority and drop precedence to packet priority (PCP) and can be bound to egress port to take effect.

  `qos profile dscp-to-dscp NAME` — Configuration in this profile allows creating user-defined mapping of DSCP and drop precedence to packet priority (DSCP) and can be bound to egress port to take effect.

Qumran supports encapsulation mapping profile to mark EXP values derived from DSCP values for IPv4 traffic and internal priority and drop precedence for tagged traffic through egress processing. EXP value encapsulation will be determined by one of the following methods:

- Default egress encapsulation mappings are configured as explained in “*Default QoS Mappings*.”
- Global egress EXP encapsulation mapping profile is available for modifying DSCP value to EXP encapsulation value for IPv4 traffic, and internal priority and drop precedence values to EXP encapsulation for tagged traffic. The command: `qos profile exp-encp default,` allows configuration of L3 DSCP to EXP mapping, and L2 queue, color to EXP mapping globally.
- User-defined egress EXP encapsulation mapping profiles can be created and bound to egress label switched port to override the global configuration: `qos profile exp-encap NAME` — configuration in this profile allows creating user-defined mapping of L3 DSCP to EXP and L2 queue, color to EXP encapsulation values and can be bound to an egress label switched port to take effect on network edge devices (Ingress LER).

CHAPTER 9 Default QoS Mappings

If a user defined profile map is not created or applied to ingress or egress traffic, Qumran uses a default map to assign PCP, DSCP, EXP priority, and drop precedence values. The following tables describe the default QoS mapping values:

Ingress decode mapping table:

- PCP, DEI-to-TC and DP table
- DSCP-to-TC and DP table
- EXP-to-TC and DP table

Egress encode mapping table:

- TC and DP-to-PCP table
- DSCP, DP-to-DSCP table
- EXP encapsulation table

Table 9-74 lists the default PCP, DEI-to-TC, and DP mappings.

Table 9-74: Default PCP, DEI-to-TC and DP

PCP (CoS)	drop eligibility (DE)	Traffic class (queue)	Drop precedence (color)
0 (000)	0	0	Green
0 (000)	1	0	Yellow
1 (001)	0	1	Green
1 (001)	1	1	Yellow
2 (010)	0	2	Green
2 (010)	1	2	Yellow
3 (011)	0	3	Green
3 (011)	1	3	Yellow
4 (100)	0	4	Green
4 (100)	1	4	Yellow
5 (101)	0	5	Green
5 (101)	1	5	Yellow
6 (110)	0	6	Green
6 (110)	1	6	Yellow
7 (111)	0	7	Green
7 (111)	1	7	Yellow

Table 9-75 lists the default TC and DP-to-PCP mappings. This table is effective when egress remarking is enabled.

Table 9-75: Default TC and DP-to-PCP

Traffic class (queue)	Drop precedence (color)	Priority (CoS/PCP)	Drop eligibility (CFI)
0	Green	0	0
0	Yellow/red	0	1
1	Green	1	0
1	Yellow/red	1	1
2	Green	2	0
2	Yellow/red	2	1
3	Green	3	0
3	Yellow/red	3	1
4	Green	4	0
4	Yellow/red	4	1
5	Green	5	0
5	Yellow/red	5	1
6	Green	6	0
6	Yellow/red	6	1
7	Green	7	0
7	Yellow/red	7	1

Note: Table information with red color is applicable only when red packet drop is disabled on the device. Otherwise, red packets are dropped by default.

Table 9-76 lists the default DSCP-to-TC, DP mappings..

Table 9-76: Default DSCP-to-TC and DP

DSCP	Traffic class (queue)	Drop precedence (color)
0 (000000 - BE/CS0)	0	Green
1 (000001)	0	Green
2 (000010)	0	Green
3 (000011)	0	Green
4 (000100)	0	Green
5 (000101)	0	Green
6 (000110)	0	Green

Table 9-76: Default DSCP-to-TC and DP (Continued)

DSCP	Traffic class (queue)	Drop precedence (color)
7 (000111)	0	Green
8 (001000 - CS1)	1	Green
9 (001001)	1	Green
10 (001010 - AF11)	1	Green
11 (001011)	1	Green
12 (001100 - AF12)	1	Yellow
13 (001101)	1	Green
14 (001110 - AF13)	1	Yellow
15 (001111)	1	Green
16 (010000 - CS2)	2	Green
17 (010001)	2	Green
18 (010010 - AF21)	2	Green
19 (010011)	2	Green
20 (010100 - AF22)	2	Yellow
21 (010101)	2	Green
22 (010110 - AF23)	2	Yellow
23 (010111)	2	Green
24 (011000 - CS3)	3	Green
25 (011001)	3	Green
26 (011010 - AF31)	3	Green
27 (011011)	3	Green
28 (011100 - AF32)	3	Yellow
29 (011101)	3	Green
30 (011110 - AF33)	3	Yellow
31 (011111)	3	Green
32 (100000 - CS4)	4	Green
33 (100001)	4	Green
34 (100010 - AF41)	4	Green
35 (100011)	4	Green

Table 9-76: Default DSCP-to-TC and DP (Continued)

DSCP	Traffic class (queue)	Drop precedence (color)
36 (100100 - AF42)	4	Yellow
37 (100101)	4	Green
38 (100110 - AF43)	4	Yellow
39 (100111)	4	Green
40 (101000 - CS5)	5	Green
41 (101001)	5	Green
42 (101010)	5	Green
43 (101011)	5	Green
44 (101100)	5	Green
45 (101101)	5	Green
46 (101110)	5	Green
47 (101111)	5	Green
48 (110000 - CS6)	6	Green
49 (110001)	6	Green
50 (110010)	6	Green
51 (110011)	6	Green
52 (110100)	6	Green
53 (110101)	6	Green
54 (110110)	6	Green
55 (110111)	6	Green
56 (111000 - CS7)	7	Green
57 (111001)	7	Green
58 (111010)	7	Green
59 (111011)	7	Green
60 (111100)	7	Green
61 (111101)	7	Green
62 (111110)	7	Green
63 (111111)	7	Green

Table 9-77 lists the default DSCP and DP-to-DSCP mapping. This table is effective when egress remarking is enabled.

Table 9-77: Default DSCP and DP-to-DSCP

DSCP	Drop precedence (color)	Out-DSCP
0 (000000 - BE/CS0)	Green/yellow/red	0 (000000 - BE/CS0)
1 (000001)	Green/yellow/red	1 (000001)
2 (000010)	Green/yellow/red	2 (000010)
3 (000011)	Green/yellow/red	3 (000011)
4 (000100)	Green/yellow/red	4 (000100)
5 (000101)	Green/yellow/red	5 (000101)
6 (000110)	Green/yellow/red	6 (000110)
7 (000111)	Green/yellow/red	7 (000111)
8 (001000 - CS1)	Green/yellow/red	8 (001000 - CS1)
9 (001001)	Green/yellow/red	9 (001001)
10 (001010 - AF11)	Green	10 (001010 - AF11)
10 (001010 - AF11)	Yellow	12 (001100 - AF12)
10 (001010 - AF11)	Red	14 (001110 - AF13)
11 (001011)	Green/yellow/red	11 (001011)
12 (001100 - AF12)	Green/yellow	12 (001100 - AF12)
12 (001100 - AF12)	Red	14 (001110 - AF13)
13 (001101)	Green/yellow/red	13 (001101)
14 (001110 - AF13)	Green/yellow/red	14 (001110 - AF13)
15 (001111)	Green/yellow/red	15 (001111)
16 (010000 - CS2)	Green/yellow/red	16 (010000 - CS2)
17 (010001)	Green/yellow/red	17 (010001)
18 (010010 - AF21)	Green	18 (010010 - AF21)
18 (010010 - AF21)	Yellow	20 (010100 - AF22)
18 (010010 - AF21)	Red	22 (010110 - AF23)
19 (010011)	Green/yellow/red	19 (010011)
20 (010100 - AF22)	Green/yellow	20 (010100 - AF22)
20 (010100 - AF22)	Red	22 (010110 - AF23)

Table 9-77: Default DSCP and DP-to-DSCP (Continued)

DSCP	Drop precedence (color)	Out-DSCP
21 (010101)	Green/yellow/red	21 (010101)
22 (010110 - AF23)	Green/yellow/red	22 (010110 - AF23)
23 (010111)	Green/yellow/red	23 (010111)
24 (011000 - CS3)	Green/yellow/red	24 (011000 - CS3)
25 (011001)	Green/yellow/red	25 (011001)
26 (011010 - AF31)	Green	26 (011010 - AF31)
26 (011010 - AF31)	Yellow	28 (011100 - AF32)
26 (011010 - AF31)	Red	30 (011110 - AF33)
27 (011011)	Green/yellow/red	27 (011011)
28 (011100 - AF32)	Green/yellow	28 (011100 - AF32)
28 (011100 - AF32)	Red	30 (011110 - AF33)
29 (011101)	Green/yellow/red	29 (011101)
30 (011110 - AF33)	Green/yellow/red	30 (011110 - AF33)
31 (011111)	Green/yellow/red	31 (011111)
32 (100000 - CS4)	Green/yellow/red	32 (100000 - CS4)
33 (100001)	Green/yellow/red	33 (100001)
34 (100010 - AF41)	Green	34 (100010 - AF41)
34 (100010 - AF41)	Yellow	36 (100100 - AF42)
34 (100010 - AF41)	Red	38 (100110 - AF43)
35 (100011)	Green/yellow/red	35 (100011)
36 (100100 - AF42)	Green/yellow	36 (100100 - AF42)
36 (100100 - AF42)	Red	38 (100110 - AF43)
37 (100101)	Green/yellow/red	37 (100101)
38 (100110 - AF43)	Green/yellow/red	38 (100110 - AF43)
39 (100111)	Green/yellow/red	39 (100111)
40 (101000 - CS5)	Green/yellow/red	40 (101000 - CS5)
41 (101001)	Green/yellow/red	41 (101001)
42 (101010)	Green/yellow/red	42 (101010)
43 (101011)	Green/yellow/red	43 (101011)

Table 9-77: Default DSCP and DP-to-DSCP (Continued)

DSCP	Drop precedence (color)	Out-DSCP
44 (101100)	Green/yellow/red	44 (101100)
45 (101101)	Green/yellow/red	45 (101101)
46 (101110)	Green/yellow/red	46 (101110)
47 (101111)	Green/yellow/red	47 (101111)
48 (110000 - CS6)	Green/yellow/red	48 (110000 - CS6)
49 (110001)	Green/yellow/red	49 (110001)
50 (110010)	Green/yellow/red	50 (110010)
51 (110011)	Green/yellow/red	51 (110011)
52 (110100)	Green/yellow/red	52 (110100)
53 (110101)	Green/yellow/red	53 (110101)
54 (110110)	Green/yellow/red	54 (110110)
55 (110111)	Green/yellow/red	55 (110111)
56 (111000 - CS7)	Green/yellow/red	56 (111000 - CS7)
57 (111001)	Green/yellow/red	57 (111001)
58 (111010)	Green/yellow/red	58 (111010)
59 (111011)	Green/yellow/red	59 (111011)
60 (111100)	Green/yellow/red	60 (111100)
61 (111101)	Green/yellow/red	61 (111101)
62 (111110)	Green/yellow/red	62 (111110)
63 (111111)	Green/yellow/red	63 (111111)

Note: Table information with red color is applicable only when red packet drop is disabled on the device. Otherwise, red packets are dropped by default.

Table 9-78 lists the default EXP-to-TC and DP mappings.

Table 9-78: Default EXP-to-TC and DP

EXP	Traffic class (queue)	Drop precedence (color)
0 (000)	0	Green
1 (001)	1	Green
2 (010)	2	Green

Table 9-78: Default EXP-to-TC and DP (Continued)

EXP	Traffic class (queue)	Drop precedence (color)
3 (011)	3	Green
4 (100)	4	Green
5 (101)	5	Green
6 (110)	6	Green
7 (111)	7	Green

Table 9-79 and Table 9-80 list the default EXP encapsulation mappings:

Table 9-79: Default EXP encapsulation table (L2 traffic)

Traffic class (queue)	Drop precedence (color)	EXP
0	Green/yellow/red	0
1	Green/yellow/red	1
2	Green/yellow/red	2
3	Green/yellow/red	3
4	Green/yellow/red	4
5	Green/yellow/red	5
6	Green/yellow/red	6
7	Green/yellow/red	7

Note: Table information with red color is applicable only when red packet drop is disabled on the device. Otherwise, red packets are dropped by default.

Table 9-80 displays the default EXP encapsulation table (L3 traffic).

Table 9-80: Default EXP encapsulation table (L3 traffic)

DSCP	EXP
0 - 7	0
8 - 15	1
16 - 23	2
24 - 31	3
32 - 39	4
40 - 47	5

Table 9-80: Default EXP encapsulation table (L3 traffic)

DSCP	EXP
48 - 55	6
56 - 63	7

CHAPTER 10 Configuring QoS

The configuration process involving several commands is described in the following chapter.

Configuring Ingress QoS Procedures

Following section explains the configuration details involved to achieve the ingress QoS treatment as explained in "Chapter 6, *Modifying Internal Priority at Ingress*" and "Chapter 7, *Remarking Packet Priority at Ingress*."

The configuration steps involved are described below:

- Configuring trust level on switch ports
- Configuring internal priority for untagged traffic on switch ports
- Configuring ingress decode mapping profile
- Binding ingress decode mapping profile
- Configuring policy-map to modify internal or packet priority

Configuring trust level on switch ports

Switch ports support two trust levels. By default, trust level is based on PCP value. However, trust level based on DSCP value is configurable per port.

Trust level to DSCP value can be configured through the command:

```
trust dscp
```

When trust DSCP is configured on the port, internal priority will be derived from DSCP value of IPv4 packet based on default `dscp-to-queue` profile configuration. Drop precedence for untagged traffic will be derived from DSCP value of IPv4 packet based on `default dscp-to-queue` profile configuration. For tagged traffic, drop precedence will continue to be based on DEI bit on the packet.

Configuring internal priority for untagged traffic on switch ports

For tagged traffic, internal priority will be derived from PCP value of the packet. Untagged traffic will not carry PCP value and are assigned with internal priority zero by default. Internal priority can be assigned to untagged traffic with following port level configuration:

```
qos untagged-priority <0-7>
```

With untagged priority configured on switch port, internal priority will be selected for untagged traffic based on the configured value.

An example of the configuration is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#qos untagged-priority 3
(config-if)#exit
```

In the example configuration, untagged traffic received on xe1 will be assigned with internal priority 3 and will be transmitted out of queue 3 at egress port.

Configuring Ingress Decode Mapping Profile

In order to modify the priority and drop precedence values used within the device, user-defined decode mapping profiles can be created or global decode mapping profile contents can be modified.

Three types of decode mapping profiles are supported based on packet priority encoded in tagged IPv4 and in MPLS traffic.

Configuring PCP-to-TC Mapping Profile

User-defined profile can be created or global profile can be modified for PCP-to-TC through the following command:

```
qos profile cos-to-queue (NAME | default)
```

Inside this command PCP-to-TC mapping can be configured using the values:

```
cos <0-7> queue <0-7>
```

Here, CoS is the PCP value and the queue value is the traffic-class being configured.

An example of the configuration is shown below:

```
(config)#qos profile cos-to-queue profile1
(config-ingress-cos-map)#cos 3 queue 4
(config-ingress-cos-map)#cos 2 queue 1
(config-ingress-cos-map)#exit
```

Note: This mapping profile is applicable only to switch ports.

Configuring DSCP-to-TC, DP, DSCP Mapping Profile

User-defined profiles can be created or global profiles can be modified for DSCP-to-TC, DP, and DSCP using the following command:

```
qos profile dscp-to-queue (NAME | default)
```

Inside this command DSCP-to-TC, DP, and DSCP mapping can be configured using the command:

```
dscp <0-63> queue <0-7> (color (green | yellow | red)|) (dscp <0-63>|)
```

An example configuration is shown below:

```
(config)#qos profile dscp-to-queue profile2
(config-ingress-dscp-map)#dscp 8 queue 2
(config-ingress-dscp-map)#dscp 25 queue 4 color yellow
(config-ingress-dscp-map)#exit
```

Note: This mapping profile is applicable only on router ports. However, the default mapping profile is applicable on switch ports as well, if trust level on the switch port is set to DSCP.

Ingress stage remarking of DSCP values can be achieved by configuring the output DSCP in the command, however, this remarking can be overwritten by policy-map based remarking or by egress remarking.

Configuring EXP-to-TC, DP Mapping Profile

Global profile can be modified for EXP-to-TC and DP through the following command:

```
qos profile exp-to-queue default
```

Inside this command, PCP-to-TC mapping can be configured using the command:

```
exp <0-7> queue <0-7> (color (green | yellow | red)|)
```

An example configuration is shown below:

```
(config)#qos profile exp-to-queue default
(config-ingress-exp-queue-map)#exp 3 queue 4 color yellow
(config-ingress-exp-queue-map)#exp 2 queue 1
(config-ingress-exp-queue-map)#exit
```

Note: This mapping profile is applicable only on label-switched router ports.

Binding Ingress Decode Mapping Profile

User-defined mapping profiles will be effective only when they are bound to ingress ports or any services.

User-defined profiles can be bound to port using the command:

```
qos map-profile (cos-to-queue | dscp-to-queue) NAME
```

An example of binding user-defined map to port is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#qos map-profile cos-to-queue profile1
```

PCP-to-TC decode profiles can be bound to VPLS service instances or attachment circuits. Profile binding to these services can be achieved using the commands:

```
vpls-qos map-profile cos-to-queue NAME
vc-qos map-profile cos-to-queue NAME
```

An example of binding a PCP-to-TC mapping profile to a VPLS service is shown below:

```
(config)#mpls vpls vpls1 1
(config-vpls)#vpls-qos map-profile cos-to-queue cq-profile-1
```

An example of binding a PCP-to-TC profile to an attachment circuit is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)# mpls-vpls MPLS-VPLS service-template VPLS-10
(config-if-vpls)#vc-qos map-profile cos-to-queue cq-profile-2
```

Profile configured on the VPLS service is effective for all attachment circuits associated with VPLS service. However, if a profile is bound to an attachment circuit, then that profile takes higher priority for that attachment circuit.

Traffic received on VPLS service will be affected by QoS treatment by configurations in the following order:

1. Set queue through policy-map configuration. Refer below section for details.
2. PCP-to-TC profile configuration bound to attachment circuit.
3. PCP-to-TC profile configuration bound to VPLS service.
4. PCP-to-TC profile configuration bound to ingress port.
5. PCP-to-TC profile configuration.

Configuring Policy-map to Modify Internal or Packet Priority

QoS policy-map frame work can be used to modify the internal priority or remark the packet priority. For policy-map configuration, refer to “Chapter 2, *Configuring a QoS Policy-map*.” Set action has following two options:

- Modify internal priority - Internal priority or traffic class can be set using the command set queue <0-7> and this command will modify only the internal priority and the configuration is not carried forward to next device.
- Remark packet priority - Packet priority can be set at the ingress processing through set cos <0-7> and set dscp <0-63> to modify PCP value for tagged traffic received on switch port and DSCP value for IPv4 traffic received on router port. Both commands implicitly modify internal priority. Value for internal priority is derived from cos-to-queue profile bound to switch port and DSCP-to-queue profile bound to router port. If profile is not explicitly bound on the interface, internal priority will be derived from default cos-to-queue profile or default dscp-to-queue profile based on interface type. On VLAN interface, set cos will update only internal priority if the traffic is routed. Even if the traffic is routed to another VLAN interface, set cos will not set the packet priority on newly constructed VLAN header and it will be 0 or subject to egress remarking configuration. If traffic is switched, then set cos on VLAN interface will update both internal priority and packet priority. Qumran doesn't support remarking on MPLS traffic.

Configuration example for modifying traffic class is shown below:

```
(config)#policy-map p-1
(config-pmap-qos)#class c-1
(config-pmap-c-qos)#set queue 5
(config-pmap-c-qos)#exit
```

The commands `set cos` and `set dscp` can be configured similarly.

Configuring Egress QoS Procedures

Following section explains the configuration details involved to achieve the egress QoS treatment as explained in "Chapter 8, *Remarking Packet Priority at Egress*."

Configuration steps involved are described below:

- Configuring egress remarking
- Configuring egress encode mapping profile
- Binding egress encode mapping profile
- Configuring and binding EXP encapsulation profile

Configuring Egress Remarking

Qumran supports remarking through egress processing. Remarking is configurable separately for tagged traffic and IPv4 traffic. Remarking can be enabled on the device through global configuration or per interface configuration. Commands provide the flexibility to configure enable remarking globally but selectively disable on certain ports or enable only on certain ports.

An example of enabling egress remarking globally is shown below:

```
(config)#qos remark cos
```

This configuration takes effect on all egress switch ports and tagged traffic transmitted through the port will be egress remarked.

The syntax of the command is:

```
qos remark (cos | dscp)
```

An example of enabling egress remarking on an egress port is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)# qos remark cos enable
```

This configuration takes effect on xe1 and tagged traffic transmitted through xe1 will be egress remarked.

The syntax of the command is:

```
qos remark (cos | dscp) (enable | disable)
```

Configuring Egress Encode Mapping Profile

In order to modify the default encoding packet priority values when remarking is enabled on the device, a user-defined encode mapping profile can be created or global decode mapping profile content can be modified.

Two types of encode mapping profiles are supported in Qumran device.

Configuring TC, DP-to-PCP mapping profile

User-defined profile can be created or global profile can be modified for TC, DP-to-PCP using the following command:

```
qos profile queue-color-to-cos (NAME | default)
```


In this profile mode TC, DP-to-PCP mapping can be configured through the command:

```
queue <0-7> (color (green | yellow)| red) cos <0-7>
```

Here, the queue value is the traffic class, color is the drop precedence, and CoS is the PCP value to be remarked.

An example of a configuration is shown below:

```
(config)#qos profile queue-color-to-cos profile1
(config-egress-cos-map)#queue 4 cos 3
(config-egress-cos-map)#queue 1 color yellow cos 2
(config-egress-cos-map)#exit
```

Note: This mapping profile is applicable only on switch ports.

Configuring DSCP, DP to DSCP mapping profile

User-defined profiles can be created or global profiles can be modified for DSCP, DP-to-DSCP using the following command:

```
qos profile dscp-to-dscp (NAME | default)
```

Inside this profile mode DSCP, DP-to-DSCP mapping can be configured using the command:

```
dscp <0-63> (color (green | yellow)| red) dscp <0-63>
```

A configuration example is shown below:

```
(config)#qos profile dscp-to-dscp profile2
(config-egress-dscp-map)#dscp 8 dscp 7
(config-egress-dscp-map)#dscp 24 color yellow dscp 30
(config-egress-dscp-map)#exit
```

Note: This mapping profile is applicable only on router ports.

Note: When ingress DSCP-to-TC, DP, or DSCP profiles with ingress DSCP remarking is bound to an ingress router port, remarked DSCP values will be input for egress DSCP and DP-to-DSCP profiles on the egress interface.

An example of this case is shown below:

```
(config)#qos profile dscp-to-queue profile1
(config-ingress-dscp-map)#dscp 10 queue 3 dscp 24
```

If this profile is bound to ingress router port, then traffic with DSCP 10 will be set with internal priority 3 and DSCP will be remarked to 24 at ingress stage.

```
(config)#qos profile dscp-to-dscp profile2
(config-egress-dscp-map)#dscp 24 dscp 30
```

If the above profile is bound to egress router port, then the mapping entry will match the traffic with remarked DSCP 24 and will effectively update the DSCP value to 30 while egressing the traffic. As a result, traffic with DSCP value 10 will be remarked to DSCP value 30.

Binding egress encode mapping profile

For user-defined mapping profiles to work, they must be bound to egress ports and egress remarking must be enabled.

User-defined profiles can be bound to ports using the following command:

```
qos map-profile (queue-color-to-cos | dscp-to-dscp) NAME
```

An example of binding a user-defined map to a port is shown below:

```
(config)#interface xe1
(config-if)#qos map-profile dscp-to-dscp profile1
```

TC and DP-to-PCP encode profiles can be bound to a VPLS service instance or attachment circuit. Profile binding to these services can be achieved using the following commands:

```
vpls-qos map-profile queue-color-to-cos NAME
vc-qos map-profile queue-color-to-cos NAME
```

An example of binding PCP-to-TC mapping a profile to a VPLS service is shown below:

```
(config)# mpls-vpls MPLS-VPLS service-template VPLS-10
(config-vpls)#vpls-qos map-profile queue-color-to-cos qc-profile-1
```

An example of binding TC, DP-to-PCP profile to attachment circuit is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#vc-qos map-profile queue-color-to-cos qc-profile-2
```

QoS egress remarking treatment on VPLS service has multiple configurations available and the priority of configuration is similar to the one explained in “Binding Ingress Decode Mapping Profile”.

Configuring and Binding EXP Encapsulation Profile

When a packet enters an MPLS network side from access side, the MPLS label will be encapsulated to the packet. Qumran supports inheriting packet priority to MPLS header from DSCP values for IPv4 traffic. For tagged traffic, packet priority is inherited by the MPLS header from the traffic class and drop precedence.

Qumran supports both global EXP encapsulation mapping profile and user-defined EXP encapsulation mapping profiles per egress port.

User-defined profiles can be created or global profile can be modified for EXP encapsulation using the following command:

```
qos profile exp-encap (NAME | default)
```

Inside this profile mode, DSCP to EXP mapping for L3 traffic and queue, color to EXP mapping for L2 traffic can be configured using the following ranges:

```
l3 dscp <0-63> exp <0-7>
l2 queue <0-7> (color (green|yellow|red)|) exp <0-7>
```

An example of binding a user-defined map to an egress port of ingress LER is shown below:

```
(config)#interface xe1
(config-if)#label-switching
(config-if)#qos map-profile exp-encap profile1
```

Note: This profile is applicable only on network facing ports of the ingress LER device.

CHAPTER 11 Displaying QoS Information

The following QoS information can be displayed:

- QoS Configuration Information – QoS configuration such as qos mapping profiles, class-maps and policy-maps can be verified by using show commands.
- QoS Packet and Byte Statistics – count of packets and bytes matching the match criteria configured in class-maps bound to ingress ports through policy-maps can be displayed when QoS statistics is enabled.

Displaying QoS Configuration Information

The QoS configurations that can be displayed are listed below:

- Mapping profile configuration
- Class-map configuration
- Policy-map configuration

Display Mapping Profile Configuration

Mapping profile configuration can be displayed using the command:

```
show qos-profile (type (cos-to-queue | dscp-to-queue | exp-to-queue | queue-color-to-cos | dscp-to-dscp | dscp-to-exp) |) (PROFILE-NAME|)
```

Refer to the "*Configuration Guide*" for detailed information of the mapping profile output.

Display Class-map Configuration

Class-map configuration can be verified with the command `show class-map (type qos|NAME|)`.

Sample output for the class-map configuration is shown below:

```
#show class-map type qos

 Type qos class-maps
 ===================
      class-map c1
         match vlan 200

      class-map type qos match-any class-default
```

Display policy-map configuration

Policy-map configuration can be verified with the command `show policy-map type qos (NAME|)`.

Sample output for the policy-map configuration is shown below:

```
#show policy-map type qos

Type qos policy-maps
====================

policy-map p1
 class c1
  police cir 2 mbps
  exit
```

Display Policy-map Configured on an Interface

Type qos policy-map configured on an interface is displayed by the command show policy-map interface INTERFACE-NAME type qos.

Sample output of this command is shown below:

```
#show policy-map interface xe1 type qos

Interface xe1
Type QoS statistics status : disabled

Service-policy (qos) input: parentPmap
---------------------------
Class-map (qos): vlan2 (match all)
 match vlan 2
 police cir 2 mbps

     Child Service-policy (qos) : childPmap
     ---------------------------
     Class-map (qos): class-default (match any)

     Class-map (qos): cos1 (match all)
      match cos 1
      police cir 1 mbps
```

To display a specific class within type qos policy-map configured on the interface use the command `show policy-map interface INTERFACE-NAME (class NAME|) type qos`.

Sample output of this command is shown below:

```
#show policy-map interface xe0 class cos1 type qos

Interface xe0

Type QoS statistics status : disabled

Class-map (qos): vlan2 (match all)
     Class-map (qos): cos1 (match all)
      match cos 1
      police cir 1 mbps
```

Displaying QoS packet and Byte Counters

QoS statistics can be enabled, displayed and cleared as described in following section:

- Enabling QoS packet and byte counters
- Displaying QoS packet and byte counters
- Clearing QoS packet and byte counters

Enabling QoS Packet and Byte Counters

Enable ingress and egress statistics using the command qos statistics as shown below.

```
(config)#qos statistics
```

The default for this command is disabled statistics.

Using no option statistics can be disabled.

Displaying QoS Packet and Byte Counters

Once statistics are enabled, type qos policy-map statistics and configurations can be displayed using the command `show policy-map interface INTERFACE-NAME type qos`.

A Sample output of this command is shown below:

```
#show policy-map interface xe0 type qos

Interface xe0

Type QoS statistics status : enabled

Class-map (qos): vlan2 (match all)
 match vlan 2
 police cir 2 mbps

     Class-map (qos): class-default (match any)
           matched      : 5503 packets, 8254500 bytes
           transmitted  : 92 packets, 138000 bytes
           dropped      : 5411 packets, 8116500 bytes

     Class-map (qos): cos1 (match all)
      match cos 1
      police cir 1 mbps
           matched      : 11010 packets, 16513500 bytes
           transmitted  : 94 packets, 141000 bytes
           dropped      : 10916 packets, 16372500 bytes
```

Statistics of type qos class-maps in the type qos policy-maps that are configured on the interfaces can be displayed using `show policy-map statistics (interface INTERFACE-NAME|) (class NAME|) type qos.`

A Sample output of this command is shown below:

```
#show policy-map statistics type qos
+---------------+----------------+----------------+----------------+-------------+
|    Class-map   |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes
|
+---------------+----------------+----------------+----------------+-------------+
xe0
 vlan2
   cos1             9012              13516500          8935              13401000
xe2
 vlan2
   class-default    4452              6678000           4302              6453000


#show policy-map interface xe0 statistics type qos
+---------------+----------------+----------------+----------------+------------+
```

```
|    Class-map   |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+-----------------+-----------------+-----------------+------------+
 vlan2
   cos1             1073131           1609695000        1063993           1595988000


#show policy-map statistics class cos1 type qos
+----------------+-----------------+-----------------+-----------------+-----------+
|    Class-map   |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+-----------------+-----------------+-----------------+-----------+
xe0
 vlan2
   cos1             1399290           2098933500        1387374           2081059500


#show policy-map int xe0 statistics class cos1 type qos
+----------------+-----------------+-----------------+-----------------+----------+
|    Class-map   |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+-----------------+-----------------+-----------------+----------+
 vlan2
   cos1             1563686           2345527500        1550370           2325553500
```

Note: In order to check statistics, QoS statistics profile need to be enabled for Qumran devices. QoS can either use ingress-acl statistics profile or ingress-qos statistics profile. When ACL groups are configured on the same interface as QoS and both ACL and QoS need explicit counters, then ingress-qos statistics profile need to be configured along with ingress-acl statistics profile. However, this will have other limitations on statistics profiles. Please refer hardware-profile statistics for more details.

Clearing QoS Packet and Byte Counters

QoS statistics can be cleared using the command `clear qos statistics`. This clears both ingress QoS and egress queuing statistics.

CHAPTER 12 Configuring Egress Queues on Ports

Every physical port of a Qumran device has eight priority queues and every subinterface has four priority queues. These ports and subinterfaces can be applied with several egress QoS parameters – these will be discussed in the next sections. (For more about subinterfaces, see Chapter 21, *Subinterface Queuing*.) When the QoS feature is enabled, all priority queues of the ports are configured with certain default egress queuing parameters.

To customize the treatment on the priority queues, the queuing policy-map infrastructure needs to be used. The following section explains the basic configuration details involved to apply queue level treatment on a port.

Configuring the Default Queuing Policy-Map

When the QoS feature is enabled, all ports of the Qumran device is supplied with a default policy-map of queuing type. The default policy-map is created with the name "`default-out-policy`" which is reserved and modifying parameters in this policy-map is reflected on all ports that do not have customized queuing policy-maps. Customized queuing policy-maps can be created and bound to ports to treat ports differently from the default configuration.

The `default-out-policy` policy-map is created with the default eight classes and the default subinterface `subif-default-out-policy` policy-map as Qumran supports eight priority queues per port and four priority queues per subinterface. Once the policy-map is configured, priority queue class-maps can be configured with the following command:

```
class type queuing default (q0|q1|q2|q3|q4|q5|q6|q7)
```

Class-maps qx represent the respective priority queuing class-maps which can be configured with different queue level parameters.

Creating a Queuing Class-Map

```
(no|) class-map type queuing NAME
```

Matching criteria: Only match queue is supported in queuing class-map for user-defined queuing policy-map.

```
(no|) match queue <0-7>
```

Note: The match queue range 0-7 is valid only for port queues classification.

For subinterface queues, the valid range is 0-3.

Creating a Queuing Policy-Map

The following is the command to create a customized default policy-map:

```
(no|) policy-map type queuing NAME
```

Binding a Queuing Policy-map

Customized queuing policy-maps take affect only when the configuration is bound to a port. Queuing policy-maps can be bound to the port with the following command:

```
service-policy type queuing output NAME
```

Where NAME represents the name of the queuing policy-map.

CHAPTER 13 Congestion Avoidance

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms, Weighted Random Early Detection (WRED) is optimum for high-speed transit networks.

Qumran supports two types of congestion avoidance mechanisms.

- Tail drop – this is the default congestion avoidance behaviour when WRED is not configured
- WRED (Weighted Random Early Detection): This is applied only when configured

Tail Drop

Tail drop treats all traffic equally and does not differentiate between classes of service. Queues get filled during period of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

Configuring Packet Drop Priority Using Tail Drop

Qumran supports configuring color independent tail drop per queue, where the default queue-limit is 62914560 bytes (~62MB). The maximum queue limit (629145600) is not guaranteed in case of congestion because this is shared memory.

```
queue-limit <1-629145600> (packets | bytes | kbytes | mbytes | ms | us)
```

no queue-limit

Tail drop configurable parameters are listed below:

- Threshold in bytes, kilobytes, megabytes, packets or millisecond format.
- Ranges of different units are as follow:
    - Packets: min 9 – max 614400
    - Bytes: min 9416 – max 629145600
    - Kilo-bytes: min 9 – max 614400
    - Mega-bytes: max 600
    - Milliseconds: max 50
    - Microseconds: max50000

An example of configuring per-priority queue Tail Drop is shown below:

```
(config)#policy-map type queuing default pq-taildrop
(config-pmap-que-def)#class type queuing default q3
(config-pmap-c-que-def)#queue-limit 1 mbytes
(config-pmap-c-que-def)#exit
```

Queue Drop Counters Verification

Drop counters with drop reason can be verified globally by using the following command:

```
#show hardware-discard-counters
+----------------------------------------+---------------+--------------+
| Registers                              | Core 0        | Core 1       |
+----------------------------------------+---------------+--------------+
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER       1596100
   Reason: VOQ_VOQ_MX_QSZ_STATUS              Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER       59807
   Reason: SRC_EQUAL_DEST_INT                 Y
```

Weighted Random Early Discard (WRED)

Qumran assigns each port eight priority queues to buffer traffic level that exceeds the port's total bandwidth. When traffic congestion persists, packets are dropped randomly. As a result traffic of greater priority may be dropped instead of traffic with lower priority.

In order to protect higher priority traffic from being dropped in such a scenarios, Qumran supports monitoring traffic congestion and drop packets based on a Weighted Random Early Discard (WRED) algorithm. Early detection of traffic congestion helps in avoiding global synchronization.

This algorithm enables the system to calculate current average queue length and compares the value against the configured minimum and maximum threshold values. Configured weight is a factor of calculating average queue length. If the calculated average queue length is within the configured minimum threshold, then the packet is enqueued. If the queue length is more than the configured maximum threshold, the packet will be dropped. When the queue length increases above minimum threshold and is within the configured maximum threshold, decision to enqueue or drop the packet is taken based on the configured drop probability. Higher drop probability packets are dropped and lower drop probability packets are enqueued.

When the current average queue length is slightly above the minimum threshold, packet drop count will be lower and increases as the current queue length reaches towards maximum threshold. Drop probability configuration decides the fraction of packet drops when average queue length reaches maximum threshold.

This method allows the application to take protective measures and synchronize the lost sessions over a period of time and thus avoiding sudden surges of traffic. Configurable parameters should be effective enough to provide enough time for the application to take corrective measures. If the gap between minimum threshold and maximum threshold values is small, then the time required for average queue length to increase from minimum threshold to maximum threshold is less and the algorithm will be ineffective.

Figure 13-119 shows how weighted random early discard works.

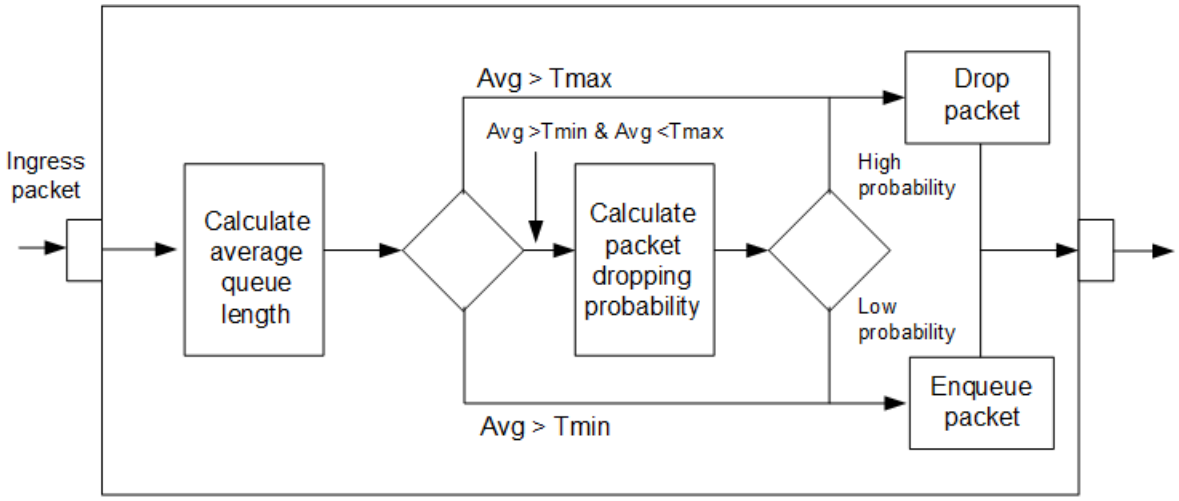


Figure 13-119: Weighted random early discard flow algorithm

Configuring Packet Drop Probability Using WRED

Qumran device supports both color independent per-priority queue WRED configuration and per-color, per-priority queue WRED configuration. One of the options is configurable per queue based on the requirement.

WRED configurable parameters are listed below:

- min_threshold: Minimal average queue size to apply WRED. Can be configured in bytes, kilobytes, megabytes, packets or millisecond format.
- max_thershold: Maximum average queue size to apply WRED. Can be configured in bytes, kilobytes, megabytes, packets or millisecond format.
- weight–factor of current size versus average size, in the calculation of new average size. Can be configured in range of 1 to 31 (optional).
- drop probability–maximum WRED drop probability applied at maximum threshold. Can be configured in percentage (optional).

At lower weight, average queue size will increase at the rate of instantaneous queue size, hence more packets will be dropped by WRED before queuing.

In this case, yellow packets are dropped more than green packets. At higher weight, average queue size will increase very slowly in comparison to instantaneous queue size, hence fewer packets will be dropped by WRED and more number packets will be queued. As a result we will observe similar results to tail drop.

Note: Formula to calculate new queue size:

NEW_AVG = OLD_AVG + (NEW_AVG-OLD_AVG) / (2 ^gain)

Formula to calculate drop probability:

Drop Probability = (AVRG_Q_SIZE-PQAVRGMINTH)/(PQAVRGMAXTH-PQAVRGMINTH) * 100%

It is recommended to use a weight value between 1 to 3 to achieve proper WRED functionality.

An example of configuring per-priority queue WRED is shown below:

```
(config)#policy-map type queuing default pq-wred
(config-pmap-que-def)#class type queuing default q3
(config-pmap-c-que-def)#random-detect 30 mbytes 500 mbytes drop-probability 50
(config-pmap-c-que-def)#exit
```

Both the minimum and maximum threshold must be configured in the same format. Thresholds can be configured in the range of 1 kilobyte to 600 megabytes or 50 milliseconds for millisecond format. In the above configuration, priority

queue q3 is configured with a minimum threshold of 30 megabytes and a maximum threshold of 500 megabytes and a drop probability of 50%.

```
random-detect (green|yellow|red|)(min-threshold|)<1-629145600>
(packets|bytes|bytes|mbytes|ms|us) (max-threshold|)<1-629145600>
(packets|bytes|kbytes|mbytes|ms|us)(drop-probability <1-100>|)
```

An example of configuring per-color, per-priority queue WRED is shown below:

```
(config)#policy-map type queuing default pq-c-wred
(config-pmap-que-def)#class type queuing default q3
(config-pmap-c-que-def)#random-detect yellow 30 mbytes 100 mbytes drop-probability 10
(config-pmap-c-que-def)#random-detect green 100 mbytes 300 mbytes drop-probability 10
(config-pmap-c-que-def)#random-detect weight 3
(config-pmap-c-que-def)#exit
```

Configuration allows minimum threshold, maximum threshold and drop probability to be configured differently for green packets and yellow packets. In the above configuration priority queue q3 will be configured with minimum threshold of 30 megabytes and maximum threshold of 100 megabytes for yellow with drop probability for 10% and minimum threshold of 100 mbps and max threshold of 300 mbps for green with drop probability of 10% for all colors along with a weight value of 3.

Follow “Chapter 12, *Configuring Egress Queues on Ports*” for complete configuration details of queuing property configuration.

Queue drop counters verification

Drop counters with drop reason can be verified globally by using the following command:

```
#show hardware-discard-counters
+-----------------------------------------+-------------+-------------+
| Registers                               | Core 0      | Core 1      |
+-----------------------------------------+-------------+-------------+
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER      1596100
   Reason: VOQ_WRED_STATUS                   Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER      59807
   Reason: SRC_EQUAL_DEST_INT                Y
```

CHAPTER 14 Scheduling

Qumran can process all traffic if it is within the capacity of the device and all traffic will be forwarded as received. When the device reaches bandwidth constraint stage, traffic becomes subject to drop as described in "Configuring Packet Drop Probability Using WRED" or traffic scheduling as described in this section. Qumran classifies packets into one of eight internal priorities. Traffic scheduling allows to selectively forward traffic according to the forwarding queue that is mapped according to one of the following algorithm:

- Strict priority-based scheduling – This scheduling ensures the higher priority traffic is serviced ahead of lower priority traffic. As a result lower priority traffic may suffer from any access.
- WFQ (Weighted Fair Queuing) weight-based scheduling – In this scheduling, some weight based bandwidth is allocated to all queues. In this scheduling, egress traffic will be served based on the configured weight distribution.
- Mixed strict and weight based scheduling – This scheduling provides a mixture of strict priority for the higher priority queues and WFQ for the remaining priority queues. In this scheduling, strict priority should always be configured from highest to lower priority queues in sequential order and WFQ scheduling should be configured from lowest priority queues to higher priority queues in sequential order.

Configuring traffic scheduling

Traffic scheduling can be configured on a per port basis. It affects the outgoing traffic when bandwidth constraints occur. In Qumran device, all the eight queues of ports will be configured with strict priority scheduling by default when QoS feature is enabled. Strict priority level will correspond to the queue number.

Scheduling algorithms are configurable per priority queues using queuing policy-map infrastructure. The following section describes how to configure different types of scheduling:

- Configuring strict priority based traffic scheduling
- Calculating the values for WFQ Weight based traffic scheduling
- Configuring WFQ weight based traffic scheduling
- Configuring mixed strict priority and weight based scheduling

Configuring Strict Priority Based Traffic Scheduling

Qumran supports strict priority algorithm with 8 levels from 0 to 7. When QoS feature is enabled, all 8 default queues will be initialized with strict priority scheduling with level corresponding to queue number. Strict priority scheduling is configurable using the priority command on the default queuing class-maps in a queuing policy-map. Configuration takes effect when the queuing policy-map is bound to the egress interface. By default, all interfaces are configured with "default-out-policy" when QoS feature is enabled.

Below, is the command to configure strict priority based scheduling:

```
priority level <0-7>
```

An example of configuring "strict priority" is shown below:

```
(config)#policy-map type queuing default pq7-strict
(config-pmap-que-def)#class type queuing default q7
(config-pmap-c-que-def)#priority level 6
(config-pmap-c-que-def)#exit
```

Queues set with higher priority value will have higher priority. If more than one queue is set with strict priority scheduling with same level value, then there will be fair queuing between those queues

Default scheduling algorithm in Qumran device is WFQ weight based traffic scheduling with weight 1. Therefore, when strict priority configuration is removed, scheduling algorithm on that queue will be reset to WFQ with default weight 1.

Calculating the Values for WFQ Weight Based Traffic Scheduling

Weighted Fair Queueing (WFQ) scheduling weight is calculated as a percentage of the port's total bandwidth using the formula:

$$\text{Weight percentage of Q(x)} = \frac{WQ(x)}{WQ0 + WQ1 + WQ2 + WQ3 + WQ4 + WQ5 + WQ6 + WQ7}$$

```
Bandwidth percentage of Q(x) = Total bandwidth of port * weight percentage of Q(x)
```

Where:

WQ(x) is the value of the priority queue for which weight is to be determined.

WQ0-WQ7 is the assigned weight values of the eight queues – for example, if the weight values q0 to q7 are assigned as 3, 10, 5, 7, 18, 4, 9 and 1, then the Weight value of q4 can be calculated using the formula:

$$\text{Weight percentage of q4} = \frac{18}{3 + 10 + 5 + 7 + 18 + 4 + 9 + 1}$$

The weight of q4 is 31.6%. Q4 will get 31.6% of the port's total bandwidth.

Note: Due to a difference in hardware rate set values, a deviation of (<4%) is expected.

The example below explains how to derive weights based on bandwidth requirement on queues.

If the bandwidth requirement of Q0 is 5%, Q1 is 10%, Q2 is 10%, Q3 is 15% and remaining bandwidth for Q4, Q5, Q6 and Q7, then the weight for individual queue can be computed as:

Q0: 5, Q1: 10, Q2: 10, Q3: 15, Q4-Q7: (100 - 5 - 10 - 10 - 15) = 60

Equally dividing weight 60 among 4 queues will result in a weight of 15 per queue. So, the weights will be:

Q0: 5, Q1: 10, Q2: 10, Q3: 15, Q4: 15, Q5: 15, Q6: 15, Q7: 15

In this case, weight values can be simplified by dividing them with common denominator 5. So, the final set of weight values for q0 to q7 will be derived to be 1, 2, 3, 3, 3, 3, 3 and 3.

Configuring WFQ Weight Based Traffic Scheduling

Set the WFQ weight based scheduling with the following configuration:

```
(config)#policy-map type queuing default pq0-3-wfq
(config-pmap-que-def)#class type queuing default q0
(config-pmap-c-que-def)# wfq-queue weight 16
(config-pmap-c-que-def)#exit
```

where:

```
wfq-queue weight <1-127>
```

Weight values can be configured in the range of 1 to 127.

Configuring Mixed Strict Priority and Weight Based Traffic Scheduling

Qumran device supports mixed scheduling option where strict priority with same or different level values can be configured on few queues along with WFQ algorithm with same or different weights configured on other default queues. Queues configured with strict priority scheduling will have a higher weight over the queues with WFQ scheduling.

An example configuration is shown below:

```
(config)#policy-map type queuing default pq-mixed
```

```
(config-pmap-que-def)#class type queuing default q0
(config-pmap-c-que-def)# wfq-queue weight 4
(config-pmap-c-que-def)#exit
(config-pmap-que-def)#class type queuing default q1
(config-pmap-c-que-def)#priority level 3
(config-pmap-c-que-def)#exit
(config-pmap-que-def)#class type queuing default q2
(config-pmap-c-que-def)# wfq-queue weight 10
(config-pmap-c-que-def)#exit
(config-pmap-que-def)#class type queuing default q3
(config-pmap-c-que-def)#priority level 4
(config-pmap-c-que-def)#exit
(config-pmap-que-def)#class type queuing default q4
(config-pmap-c-que-def)# wfq-queue weight 30
(config-pmap-c-que-def)#exit
```

Classes 5 to 7 will be strict priority with corresponding level if these classes were not altered.

Follow “Chapter 12, *Configuring Egress Queues on Ports*” for complete configuration details of queuing property configuration.

Scheduling may be affected by resource exhaustion in case of multicast traffic.

Resource exhausted can be verified through drop reason as “RESOURCE_ERROR_STATUS.”

Queue drop counters verification

Drop counters with drop reasons can be verified globally using the command:

```
#show hardware-discard-counters
+---------------------------------+--------+--------+
| Registers                       | Core 0 | Core 1 |
+---------------------------------+--------+--------+
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER        1596100
   Reason:  RESOURCE_ERROR_STATUS               Y
            VOQ_MX_QSZ_STATUS                   Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER        59807
      Reason: SRC_EQUAL_DEST_INT                Y
```

CHAPTER 15 Egress Port and Priority Rate Shaping

Rate shaping is a method of regulating traffic rate to ensure a certain level of network performance. The difference between policing and rate shaping is that policing drops the excess traffic. Shaping buffers the excess traffic and thus insures a uniform pattern of traffic egressing. Shaping is required when the nature of traffic is busty and needs to be smoothened.

Qumran supports configuring rate shaping per priority queue or per port.

Configuring port-based rate shaping

With Port based rate shaping, total traffic can be limited to the shape rate within the limits of port bandwidth. Qumran supports per-port rate shaping configuration within a range of 52kbps to 1000gbps. The shape rate granularity of the port shaper is 52kbps.

Note: Port based shaping is supported only on physical interfaces.

```
(config)#interface xe1
(config-if)#shape rate 200 mbps
(config-if)#exit
Syntax:
shape rate <1-1000000000> (kbps|mbps|gbps)
```

Configuring priority-based rate shaping

Priority based rate shaping ensures a traffic shaping per priority queue traffic. Priority based rate shaping is configured on the queuing class-map representing priority queue. Shaping can be configured in absolute value or in percentage of bandwidth. Qumran supports per-queue rate shaping configuration within a range of 469kbps to 483gbps. Granularity is 469 Kbps for low range and 1.56% for higher range.

The following example shows a sample configuration of priority based rate shaping:

```
(config)#policy-map type queuing default pq
(config-pmap-que-def)#class type queuing default q3
(config-pmap-c-que-def)#shape 10 mbps
(config-pmap-c-que-def)#exit
```

The general syntax is::

```
shape <1-483000000> (kbps|mbps|gbps) | percent <1-100>)
```

Follow “Chapter 12, *Configuring Egress Queues on Ports*.” for complete configuration details of queuing property configuration.

Queue drop counters verification

Drop counters with drop reasons can be verified globally by using the command:

```
#show hardware-discard-counters
+---------------------------------+--------+--------+
| Registers                       | Core 0 | Core 1 |
+---------------------------------+--------+--------+
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER        1596100
   Reason: VOQ_MX_QSZ_STATUS                   Y
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER        59807
```

```
      Reason: SRC_EQUAL_DEST_INT                  Y
```

CHAPTER 16 Display Queuing Information

The following queuing information can be displayed:

- Queuing Configuration Information
- Queuing Packet and Byte Statistics

Displaying queuing configuration information

The queuing configurations that can be displayed are:

- Policy-map configuration
- Interface level queuing configuration

Display Policy-map Configuration

Use the following command to verify configurations on policy-map:

```
show policy-map (type queuing|NAME|)
```

NAME is an optional parameter which allows verifying a particular policy-map. Qumran supports only default queuing policy-maps.

Sample output for queuing policy-map configuration is shown below:

```
#show policy-map pq1

Type queuing policy-maps
========================

policy-map type queuing default pq1
 class type queuing default q0
  shape percent 60
  wfq-queue weight 20
  exit
 class type queuing default q1
  shape percent 20
  wfq-queue weight 50
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
 class type queuing default q6
  priority level 6
```

```
  exit
 class type queuing default q7
  priority level 7
  exit
```

Interface level queuing configuration

The following command shows the configuration on eight priority queues of an interface:

```
show queuing interface INTERFACE-NAME
```

Sample output of interface based queue configuration is shown below:

```
#show queuing interface xe1

Egress Queuing for Ethernet xe1 [System]
------------------------------------------------------
L0   L1   L2   Group   PrioLevel  Shape      Bandwidth
------------------------------------------------------
q0             -       -          60 percent     -
q1             -       -          20 percent     -
q2             -       High       -              -
q3             -       High       -              -
q4             -       High       -              -
q5             -       High       -              -
q6             -       High       -              -
q7             -       High       -              -
```

Display Type Queuing Policy-map Configuration and Statistics on an Interface

Type queuing policy-map configurations and statistics can be displayed using the command:

```
show policy-map interface INTERFACE-NAME type queuing
```

Sample output is shown below:

```
#show policy-map interface xe0 type queuing

Interface xe0
Type Queuing policy-map : pq1

Class-map (queuing): class-default-q
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 0
      Output
         Total        : 14303226 packets, 21454839000 bytes
         Green        : 14303226 packets, 21454839000 bytes
         Yellow       : 0 packets, 0 bytes
 match queue 1
 match queue 2
 match queue 3
 match queue 4
```

```
 match queue 5
 match queue 6
 match queue 7


Class-map (queuing): service3
 match service-template v3
 shape 1000000 kbps (inherited)
 wfq-queue weight 1

     Class-map (queuing): class-default-q
      shape 1000000 kbps (inherited)
      wfq-queue weight 1

     Class-map (queuing): data
      shape 1000000 kbps (inherited)
      wfq-queue weight 1
      queue-limit 1253376 bytes/10 ms (default)
      match queue 0
      match queue 1
           Output
              Total        : 4717105 packets, 7075660500 bytes
              Green        : 4717122 packets, 7075684500 bytes
              Yellow       : 0 packets, 0 bytes
           Rate            : 118443.625 kbps
      match queue 2
```

Configurations and statistics of a particular class in the type queuing policy-map on an interface can be displayed using the command `show policy-map interface INTERFACE-NAME (class NAME|) type queuing`

Sample output is shown below:

```
#show policy-map interface xe2 class service3

Interface xe2
Type Queuing policy-map : pq1

Class-map (queuing): service3
 match service-template v3
 shape 1000000 kbps (inherited)
 wfq-queue weight 1

     Class-map (queuing): class-default-q
      shape 1000000 kbps (inherited)
      wfq-queue weight 1
      queue-limit 1253376 bytes/10 ms (default)
      match queue 2
           Output
              Total        : 111200 packets, 166801500 bytes
              Green        : 111209 packets, 166813500 bytes
              Yellow       : 0 packets, 0 bytes
```

```
      Rate            : 59141.176 kbps
 match queue 3

Class-map (queuing): data
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 0
 match queue 1
      Output
         Total        : 222450 packets, 333678000 bytes
         Green        : 222466 packets, 333702000 bytes
         Yellow       : 0 packets, 0 bytes
      Rate            : 118287.391 kbps
```

CHAPTER 17 Display Queue Level Packet and Byte Counters

Queue level statistics can be displayed and cleared as described in the following section:

- Displaying queuing class configuration and queue packet and byte counters
- Clearing queue level packet and byte counters

Queue level statistics can be displayed using the command:

`show policy-map (interface INTERFACE-NAME|) statistics (class CLASS-NAME|) type queuing` and

`show interface (INTERFACE-NAME|) counters queue-stats`.

Sample output is shown below:

```
#show policy-map statistics type queuing
+----------------+----------------+----------------+----------------+--------------+
|     Class-map  |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+----------------+----------------+----------------+--------------+
xe0
 q1                1142             1713000          133978            200965500
 q3                1138             1707000          66451             99675000
xe2
 q1                1133             1699500          134476            201715500
 q2                1155             1732500          66655             99984000
#show policy-map statistics class q1 type queuing
+----------------+----------------+----------------+----------------+--------------+
|     Class-map  |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+----------------+----------------+----------------+--------------+
xe0
 q1                5110             7665000          598853            898278000
xe2
 q1                5084             7627500          598821            898231500
#show policy-map int xe0 statistics type queuing
+----------------+----------------+----------------+----------------+--------------+
|     Class-map  |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+----------------+----------------+----------------+--------------+
 q1                5943             8914500          697242            1045861500
 q3                5925             8887500          345696            518542500
#show policy-map int xe0 statistics class q1 type queuing
+----------------+----------------+----------------+----------------+--------------+
|     Class-map  |    Total pkts   |   Total bytes   |   Dropped pkts  |   Dropped Bytes
|
+----------------+----------------+----------------+----------------+--------------+
 q1                7314             10971000         858974            1288461000
```

Sample output for interface based queue statistics is shown below:

```
#show interface xe1 counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
```

```
+---+------+--------+---------+---------+-----------+
| Q | Q-Sz | Tx pkt | Tx byte | Drp pkt | Drop byte |
+---+------+--------+---------+---------+-----------+
q0   629160 100      12000       0         0
q0   629160 0        0           0         0
q0   629160 0        0           0         0
q0   629160 0        0           0         0
q0   629160 0        0           0         0
q0   629160 0        0           0         0
```

Display Queue Level Instantaneous Transmission Rate

The instantaneous rate at which packets are de queued/transmitted from the queues can be displayed using

`show policy-map (interface INTERFACE-NAME|) statistics (class CLASS-NAME|) type queuing (rate (kbps|mbps|gbps)|)`

Sample output of the command is shown below:

```
#show policy-map statistics type queuing rate mbps
+------------------------+----------------+
|            Class-map   | Rate (in mbps) |
+------------------------+----------------+
xe0
 q1                              1.031
 q3                              1.031
xe2
 q1                              1.031
 q2                              0.824


#show policy-map interface xe0 statistics type queuing rate mbps
+------------------------+---------------+
|            Class-map   | Rate (in mbps)|
+------------------------+---------------+
 q1                              0.700
 q3                              1.168


#show policy-map interface xe0 statistics class q1 type queuing rate mbps
+-----------------------+----------------+
|            Class-map  | Rate (in mbps) |
+-----------------------+----------------+
 q1                              0.937
```

Clearing Queue Level Packet and Byte Counters

Queue statistics can be cleared using the command:

```
clear qos statistics (interface INTERFACE-NAME |) output type queuing
```

and

```
clear interface counters.
```

CHAPTER 18 VLAN Service Queuing (VLAN Shaping)

In Qumran device, every port has default eight priority queues that can be applied. Whenever QoS feature is enabled, all priority queues of the ports will be configured with certain default egress queuing parameters. In order to customize the treatment on the priority queues, queuing policy-map infrastructure need to be used.

Service Queuing refers to mapping services to specific vlans and shaping each vlan based traffic. Within the vlan, queues can be grouped and shaped independently.

Configuring VLAN Shaping

The following section explains the configuration of basic infrastructure to provide the functionality of queuing per services on an interface. These queues will support all the possible QoS treatment via egress queuing policy-map configurations. Services can be mapped using service-template or via match vlan. Whenever we will be matching a service in a class inside a policy and attach it on interface, 4 new queues will be created for these services. User can create max 3-level scheduling hierarchy for each of the services using these policy-maps.

Policy-map attached to interface will be referred as "L0" level policy-map. Each child policy-map that will be added, will be at one incremented level i.e. L0-level's child policy-map will be L1 level policy-map and L1-level's child will be L2 policy-map. This is the max 3-level hierarchy supported in user defined policy-map.

Class-default-q is a self-created class map as part a policy map. There are two types of class-default-q CMAPs:

- When a policy is applied on an interface, the class-default-q represents the port default queues. If the operator wants to shape or apply certain TailDrop/WRED properties on the port queues, it has to be applied on the class-default-q cmap at Level 0.
- When a child policy is attached to a cmap with some service match criteria (match service-template/vlan), the class-default-q cmap in the child policy represents the queues which are left unmatched in rest of the cmaps of the child policy.

Configuring a Queuing Policy-map

When QoS feature is enabled, all ports in the Qumran device will be applied with a default policy-map of queuing type. The default policy-map is created with the name “default-out-policy” which is reserved and modifying parameters in this policy-map will reflect on all ports which don't have customized queuing policy-map. Customized queuing policy-maps can be created and bound to ports to treat ports differently from default configuration.

Creating a user-defined queuing policy-map

Qumran device supports creation of customized policy-map in which new four queues can be configured for each services. If any priority queue class-map is not configured, default behavior among these new queues is weighted fair queuing. New queues and port default queues will also have weighted fair queuing between them as default behavior.

The following command is used to create a class-map:

```
(no|) class-map type queuing NAME
```

These class-maps will be matching some services for which new queues will be created. These classes can be empty classes in order to create hierarchy and club services in a hierarchy.

Matching criteria of a queuing class-map

Queuing class-map can have four matching criteria:

1. queue: queue selection

   ```
   CLI:  (no|) match queue <0-7>
   ```

   Note: match queue range 0-7 is valid only for port queues classification.

   For service queues, valid range is 0-3.

2. service-template: service related classification

   ```
   CLI: (no|) match service-template NAME
   ```

3. vlan: list VLAN ID

   ```
   CLI:  (no|) match vlan <1-4094>
   ```

4. interface: interface name

   ```
   CLI: (no|) match interface IFNAME
   ```

   Note: The interface name can be either vlan interface or subinterface.

The following is the command to create a customized policy-map:

```
(no|) policy-map type queuing NAME
```

Once the policy-map is configured, the queuing class-maps can be configured with following command:

```
(no|) class type queuing NAME
```

Binding/Unbinding a QoS Policy-map on an Interface

Customized queuing policy-maps take affect only when the configuration is bound to a port.

Queuing policy-maps can be bound/unbound to the out-port with following command:

```
(no|) service-policy type queuing output NAME
```

Where “NAME” represents the name of the queuing policy-map.

Binding/Unbinding a QoS Policy-map as a Child Service Policy

A policy-map can be configured as a child policy in order to create a hierarchy. Queuing policy-maps can be bound to a policy-map as a child policy with following command:

```
(no|) service-policy NAME
```

Where NAME represents the name of the queuing policy-map.

Note: Child policy needs to be attached to a parent policy-map inside a class.

For example:

```
class-map type queuing data
 match queue 0
!
class-map type queuing service1
 match service-template ETH-2016
!
class-map type queuing service2
 match service-template ETH-2017
```



```
!
class-map type queuing signal
 match queue 3
!
class-map type queuing voice
 match queue 1
!
policy-map type queuing configPolicy1
 class type queuing class-default-q
  exit
 class type queuing data
  exit
 class type queuing signal
  exit
 class type queuing voice
  exit
!
policy-map type queuing customer1
 class type queuing service1
  service-policy configPolicy1
class type queuing class-default-q
  exit
!
interface xe11
 service-policy type queuing output customer1
```

Here, “customer1” is L0-level policy-map and “configPolicy1” is L1-level policy-map. Policy-map “customer1” is having a class-default-q which is having port default queues. Policy-map “configPolicy1” is having class-default-q which is representing remaining queue i.e. queue 2 as queue3 is mapped to class signal, queue1 is mapped to class voice and queue0 is mapped to class data.

WRED and taildrop configuration is applicable only in the class in which queues are mapped. If in a policy-map having a class matching the service is not having any child policy-map, then all the new queues will be mapped to the same class and WRED and taildrop configuration is valid for this class. If the class matching service is having child policy matching queues, then WRED and taildrop is valid for the child service-policy only.

Policy-map having classes matching the queues can only be configured as a child service-policy inside a class matching service or at L0 class-default-q. It cannot be attached on an interface directly

If the user-defined child service policy is applied matching queues in L0 class-default-q which are mapping port queues, supported match queue range is 0-7.

For service queues, valid range is 0-3 as only 4 new queues are created for each service.Since the queues created are 4, 8 traffic classes are mapped implicitly to 4 queues as shown in Table 18-81.

Table 18-81: Traffic class to queue mapping

Traffic class	Queue
0	0
1, 2, 3	1
4, 5	2
6, 7	3

Ingress mapping profile like cos-to-queue, dscp-to-queue, and exp-to-queue actually maps packet fields (cos/dscp/exp) to 8 traffic classes. These traffic classes are mapped one-to-one when we have 8 queues in case of physical port and to 4 queues in case of services as shown above.

Until the child service-policy is applied on L0 class-default-q (port queues), port queues will follow default mapping profiles.

QoS feature must be enabled to configure policy-maps. This infrastructure contains two entities - class-map and policy-map. Class-map holds the match criteria and class-maps can be bound to policy-map to configure QoS treatment for the matching traffic.

The following section explains the basic configuration details involved to apply queue level treatment on the port.

Note: Please refer to *MPLS configuration guide* for service-template configurations.

```
(config)# class-map type queuing customer1
(config-cmap-que)# match service-template customer1Vlan
(config-cmap-que)#exit
(config)# class-map type queuing customer2
(config-cmap-que)# match service-template customer2Vlan
(config-cmap-que)#exit
(config)# class-map type queuing customer3
(config-cmap-que)# match service-template customer3Vlan
(config-cmap-que)#exit
(config)# class-map type queuing customer4
(config-cmap-que)# match service-template customer4Vlan
(config-cmap-que)#exit

(config)#class-map type queuing data
(config-cmap-que)# match queue 0
(config-cmap-que)# exit
(config)#class-map type queuing voice
(config-cmap-que)# match queue 1
(config-cmap-que)#exit
(config)# class-map type queuing signaling
(config-cmap-que)# match queue 3
(config-cmap-que)# exit

(config)#class-map type queuing area1
(config-cmap-que)# exit
(config)#class-map type queuing area2
(config-cmap-que)# exit

(config)#policy-map type queuing traffic_policy
(config-pmap-que)# class type queuing data
(config-pmap-c-que)# shape 10 mbps
(config-pmap-c-que)# exit
(config-pmap-que)# class type queuing voice
(config-pmap-c-que)# exit
(config-pmap-c-que)# shape 2 mbps
(config-pmap-que)# class type queuing signaling
(config-pmap-c-que)# exit
(config-pmap-c-que)# shape 1 mbps
(config-pmap-c-que)# exit
```



```
(config-pmap-que)#policy-map type queuing area1_policy
(config-pmap-que)# class type queuing customer1
(config-pmap-c-que)# shape 12 mbps
(config-pmap-c-que)# service-policy traffic_policy
(config-pmap-c-que)# exit
(config-pmap-que)# class type queuing customer2
(config-pmap-c-que)# shape 12 mbps
(config-pmap-c-que)# exit

(config-pmap-que)#policy-map type queuing area2_policy
(config-pmap-que)# class type queuing customer3
(config-pmap-c-que)# shape 12 mbps
(config-pmap-c-que)# service-policy traffic_policy
(config-pmap-c-que)# exit
(config-pmap-que)# class type queuing customer4
(config-pmap-c-que)# shape 12 mbps
(config-pmap-c-que)# exit

(config-pmap-que)#policy-map type queuing xe16_policy

(config-pmap-que)# class type queuing area1
(config-pmap-c-que)# shape 100 mbps
(config-pmap-c-que)# service-policy area1_policy
(config-pmap-c-que)# exit
(config-pmap-que)# class type queuing area2
(config-pmap-c-que)# shape 100 mbps
(config-pmap-c-que)# service-policy area2_policy
(config-pmap-c-que)# exit

(config-pmap-que)#interface xe16
(config-if)# service-policy type queuing output xe16_policy
(config-if)#exit
```

Displaying Policy-map Configuration

The following is an example of `show policy-map interface` command:

```
(config)#show policy-map interface xe16

Interface xe16
Type QoS statistics status : enabled

Service-policy (queuing) output: xe16_policy
Interface Bandwidth 1000000 kbps
-----------------------------------
Class-map (queuing): area1
 shape 100 mbps
 wfq-queue weight 1

     Service-policy (queuing) output: area1_policy
     ---------------------------------
```

```
     Class-map (queuing): customer1
      match service-template customer1Vlan
      shape 12 mbps
      wfq-queue weight 1

          Service-policy (queuing) output: traffic_policy
          ----------------------------------
          Class-map (queuing): class-default-q
           shape 12000 kbps (inherited)
           wfq-queue weight 1
           queue-limit 15040 bytes/10 ms (default)
           match queue 1

          Class-map (queuing): data
           shape 10 mbps
           wfq-queue weight 1
           queue-limit 12544 bytes/10 ms (default)
           match queue 0
           Output
         Total        : 66681 packets, 66681000 bytes
         Green        : 66681 packets, 66681000 bytes
         Yellow       : 0 packets, 0 bytes

          Class-map (queuing): signaling
           shape 1 mbps
           wfq-queue weight 1
           queue-limit 9472 bytes/76 ms (default)
           match queue 3

          Class-map (queuing): voice
           shape 2 mbps
           wfq-queue weight 1

           queue-limit 9472 bytes/38 ms (default)
           match queue 2
     Class-map (queuing): customer2
      match service-template customer2Vlan
      shape 12 mbps
      wfq-queue weight 1
      queue-limit 15040 bytes/10 ms (default)
      match queue 0
      match queue 1
      match queue 2
      match queue 3

Class-map (queuing): area2
 shape 100 mbps
 wfq-queue weight 1

     Service-policy (queuing) output: area2_policy
```

```
     ------------------------------------
     Class-map (queuing): customer3
      match service-template customer3Vlan
      shape 12 mbps
      wfq-queue weight 1
      queue-limit 15040 bytes/10 ms (default)
      match queue 0
      match queue 1
      match queue 2
      match queue 3

     Class-map (queuing): customer4
      match service-template customer4Vlan
      shape 12 mbps
      wfq-queue weight 1

          Service-policy (queuing) output: traffic_policy
          -----------------------------------
          Class-map (queuing): class-default-q
           shape 12000 kbps (inherited)
           wfq-queue weight 1
           queue-limit 15040 bytes/10 ms (default)
           match queue 1

          Class-map (queuing): data

           shape 10 mbps
           wfq-queue weight 1
           queue-limit 12544 bytes/10 ms (default)
           match queue 0
          Class-map (queuing): signaling
           shape 1 mbps
           wfq-queue weight 1
           queue-limit 9472 bytes/76 ms (default)
           match queue 3

          Class-map (queuing): voice
           shape 2 mbps
           wfq-queue weight 1
           queue-limit 9472 bytes/38 ms (default)
           match queue 2

Class-map (queuing): class-default-q
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 0
 match queue 1
 match queue 2
 match queue 3
```

```
 match queue 4
 match queue 5
 match queue 6
 match queue 7
```

QoS Configuration on User-defined Policy-map

All the queuing configurations such as WRED, taildrop, WFQ, shaping are same for user-defined policy as they are in default-policy-map except the priority queue configuration.

In default-policy-map, max priority supported is 8 i.e. 0-7, while in user-defined policy-map, max priority level is 4, i.e.0-3.

Priority class will always have priority over weighted class in default policy. But in user-defined policy, when all the 4 priorities are assigned with weighted classes, priority 0 class will be in fair queuing with the total weighted queues. If 3 or less than 3 priority class are present with weighted classes, than priority class will have priority over weighted class.

For example:

```
(config-pmap-que)#policy-map type queuing area2_policy
 (config-pmap-que)# class type queuing customer1
 (config-pmap-c-que)# priority level 0
 (config-pmap-c-que)# service-policy traffic_policy
 (config-pmap-que)# class type queuing customer2
 (config-pmap-c-que)# priority level 1
 (config-pmap-c-que)# service-policy traffic_policy
 (config-pmap-que)# class type queuing customer3
 (config-pmap-c-que)# priority level 2
 (config-pmap-c-que)# service-policy traffic_policy
 (config-pmap-que)# class type queuing customer4
 (config-pmap-c-que)# priority level 3
 (config-pmap-c-que)# service-policy traffic_policy
 (config-pmap-que)# class type queuing customer5
 (config-pmap-c-que)# wfq-queue weight 1
 (config-pmap-c-que)# service-policy traffic_policy
  (config-pmap-que)# class type queuing customer6
 (config-pmap-c-que)# wfq-queue weight 2
 (config-pmap-c-que)# service-policy traffic_policy
```

In this case, customer4 will have the highest priority, while 50% of the remaining bandwidth after distributing among priority classes will be used by Customer1, and the remaining 50% will be shared by Customer5 and Customer6 (FQ between priority 0 and weighted class).

If there are only three priority classes, for example:

```
(config-pmap-que)#policy-map type queuing area2_policy
(config-pmap-que)# class type queuing customer1
(config-pmap-c-que)# priority level 0
(config-pmap-c-que)# service-policy traffic_policy
(config-pmap-que)# class type queuing customer2
(config-pmap-c-que)# priority level 1
(config-pmap-c-que)# service-policy traffic_policy
(config-pmap-que)# class type queuing customer3
(config-pmap-c-que)# priority level 2
(config-pmap-c-que)# service-policy traffic_policy
```



```
(config-pmap-que)# class type queuing customer4
(config-pmap-c-que)# wfq-queue weight 1
(config-pmap-c-que)# service-policy traffic_policy
(config-pmap-que)# class type queuing customer5
(config-pmap-c-que)# wfq-queue weight 2
(config-pmap-c-que)# service-policy traffic_policy
```

Here, Customer3 has the highest priority. Customer1 has priority 0 and will have priority over Custimer4 and Customer5.

Configuration Considerations

- Max 3 level of user defined hierarchy is supported.
- Class-default-q is a self-created class map as part a policy map. It cannot be created nor be destroyed. It will be displayed (on whichever level applicable) only when user access it. Executing command "no class-default-q", will un-configure all the configurations of class-default-q.
- User can configure all queuing parameters like weight, priority, queue-limit, wred and shape in a class inside policy.
- Queue-limit and wred is only applicable in class matching queues.
- Same service should not be matched twice in the same hierarchy at any level.
- Policy-map with classes matching queues can only be attached to the policy-map having classes with match service or L0 class-default-q class.
- Child service policy is not allowed in class matching queues unless it is L0 class-default-q.
- If a service-policy is configured as a child policy in any hierarchy, then it cannot be attached on an interface directly and vice-versa.
- All the classes inside a policy-map should have same matching criteria but not same matching criteria value.
- Class-default-q class will only be present at L0 level or at the last level in a hierarchy. Class-default-q class will be matching port default queues if the class is of L0. Class-default-a class will be matching remaining queues in the newly created queue bundle if not matched in a class.
- Valid match queue range for classifying port-queues is 0-7. For service queue it is 0-3.
- Update is possible in the policy-map except the update of match criteria. Once the class with some match criteria is used in a policy-map, it cannot be updated.
- Max 4 priority queues are supported in non-default queuing policy-map.
- VLAN shaping is only supported for L2VPN, L3VPN, and provider-bridging services.

Service Queuing refers to mapping services to specific vlans and shaping each vlan based traffic. Within the vlan, queues can be grouped and shaped independently.

Matching of traffic can be based on different parameters such as service-template, VLAN, sub interface/VLAN interface.

Below, are different configuration for L2VPN, VPLS/VPWS services, L3VPN with sub and VLAN interfaces, and a provider bridge configuration.

L2VPN- VPLS

Figure 18-120 displays a six node topology configured with end to end connectivity from Router 1 to Router 6. The end to end connectivity is established by configuring OSPF, iBGP and LDP configuration in all the routers. We should be able to ping each device from other device from topology. Configure L2VPN- VPLS services on RTR1 and RTR6 and create Qos configuration on RTR6 and verify service queuing.

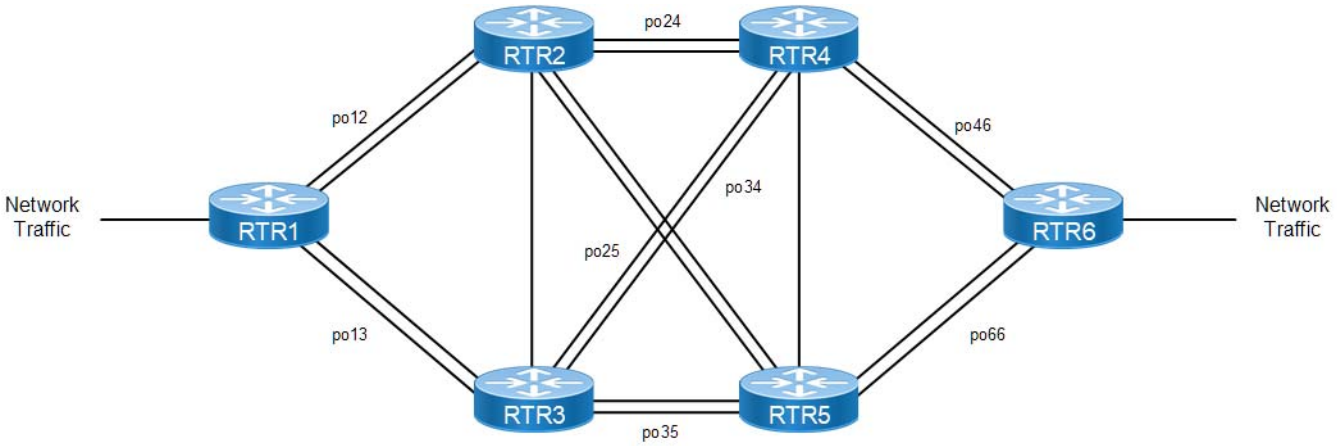


Figure 18-120: Simple Topology

RTR1

`RTR1#configure terminal`	Enter into configuration mode
`RTR1(config)#service-template VPLS-30`	Create L2VPN VPLS service template of VPLS-30
`RTR1(config-svc)# match double-tag outer-vlan 30 inner-vlan 2030`	Match for double tagged VLAN with inner VLAN 30 and outer VLAN 2030
`RTR1(config-svc)#rewrite ingress pop outgoing-tpid dot1.q`	Rewrite ingress pop outgoing as dot1q
`RTR1(config-svc)#exit`	Exit
`RTR1(config)#service-template VPLS-40`	Create L2VPN VPLS service template of VPLS-40
`RTR1(config-svc)#match double-tag outer-vlan 40 inner-vlan 2040`	Match for double tagged VLAN with inner VLAN 40 and outer VLAN 2040
`RTR1(config-svc)#rewrite ingress pop outgoing-tpid dot1.q`	Rewrite ingress pop outgoing as dot1q
`RTR1(config-svc)#exit`	Exit
`RTR1(config)#mpls vpls V30 30`	Create MPLS VPLS with V30 and 30
`RTR1(config-vpls)#service-tpid dot1.ad`	Make service tpid as dot1.ad
`RTR1(config-vpls)#signaling ldp`	Configure signaling as ldp
`RTR1(config-vpls-sig)#vpls-type vlan`	Configure vpls type as vlan
`RTR1(config-vpls-sig)#vpls-peer 6.6.6.6`	Configure peer as 6.6.6.6
`RTR1(config-vpls-sig)#exit-signaling`	Exit
`RTR1(config-vpls)#exit`	Exit
`RTR1(config)#mpls vpls V40 40`	Create MPLS VPLS with V40 and 40
`RTR1(config-vpls)#service-tpid dot1.ad`	Make service tpid as dot1.ad
`RTR1(config-vpls)#signaling ldp`	Configure signaling as LDP
`RTR1(config-vpls-sig)#vpls-type vlan`	Configure VPLS type as VLAN
`RTR1(config-vpls-sig)#vpls-peer 6.6.6.6`	Configure peer as 6.6.6.6
`RTR1(config-vpls-sig)#exit-signaling`	Exit
`RTR1(config-vpls)#exit`	Exit
`RTR1(config)#interface xe14`	Enter interface configuration

RTR1(config-if)#switchport	Change port as switchport
RTR1(config-if)#load-interval 30	Configure load interval as 30
RTR1(config-if)#mpls-vpls V30 service-template VPLS-30	Bind MPLS VPLS V30 with service template VPLS-30
RTR1(config_if_vpls)#ac-admin-status up	Change admin status as UP
RTR1(config_if_vpls)#exit-if-vpls	Exit
RTR1(config-if)#mpls-vpls V40 service-template VPLS-40	Bind MPLS VPLS V40 with service template VPLS-40
RTR1(config_if_vpls)#ac-admin-status up	Change admin status as UP
RTR1(config_if_vpls)#exit-if-vpls	Exit
RTR1(config)#router bgp 64512	Configure BGP of as number 64512
RTR1(config-router)#address-family l2vpn vpls	Enter into l2vpn VPLS address family
RTR1(config-router-af)#neighbor 6.6.6.6 activate	Activate neighbor 6.6.6.6
RTR1(config-router-af)#exit-address-family	Exit
RTR1(config-router)#exit	Exit

RTR6

RTR6#configure terminal	Enter into configuration mode
RTR6(config)#service-template VPLS-30	Create L2VPN VPLS service template of VPLS-30
RTR6(config-svc)#match double-tag outer-vlan 30 inner-vlan 2030	Match for double tagged VLAN with inner VLAN 30 and outer VLAN 2030
RTR6(config-svc)#rewrite ingress pop outgoing-tpid dot1.q	Rewrite ingress pop outgoing as dot1q
RTR6(config-svc)#exit	Exit
RTR6(config)#service-template VPLS-40	Create L2VPN VPLS service template of VPLS-40
RTR6(config-svc)#match double-tag outer-vlan 40 inner-vlan 2040	Match for double tagged VLAN with inner VLAN 40 and outer VLAN 2040
RTR6(config-svc)#rewrite ingress pop outgoing-tpid dot1.q	Rewrite ingress pop outgoing as dot1q
RTR6(config-svc)#exit	Exit
RTR6(config)#mpls vpls V30 30	Create MPLS VPLS with V30 and 30
RTR6(config-vpls)#service-tpid dot1.ad	Make service tpid as dot1.ad
RTR6(config-vpls)#signaling ldp	Configure signaling as LDP
RTR6(config-vpls-sig)#vpls-type vlan	Configure VPLS type as VLAN
RTR6(config-vpls-sig)#vpls-peer 1.1.1.1	Configure peer as 1.1.1.1
RTR6(config-vpls-sig)#exit-signaling	Exit
RTR6(config-vpls)#exit	Exit
RTR6(config)#mpls vpls V40 40	Create MPLS VPLS with V40 and 40
RTR6(config-vpls)#service-tpid dot1.ad	Make service tpid as dot1.ad
RTR6(config-vpls)#signaling ldp	Configure signaling as LDP
RTR6(config-vpls-sig)#vpls-type vlan	Configure VPLS type as VLAN

`RTR6(config-vpls-sig)#vpls-peer 1.1.1.1`	Configure peer as 1.1.1.1
`RTR6(config-vpls-sig)#exit-signaling`	Exit
`RTR6(config-vpls)#exit`	Exit
`RTR6(config)#interface xe13`	Enter interface configuration
`RTR6(config-if)#switchport`	Change port as switchport
`RTR6(config-if)#load-interval 30`	Configure load interval as 30
`RTR6(config-if)#mpls-vpls V30 service-template VPLS-30`	Bind MPLS VPLS V30 with service template VPLS-30
`RTR6(config_if_vpls)#ac-admin-status up`	Change admin status as UP
`RTR6(config_if_vpls)#exit-if-vpls`	Exit
`RTR6(config-if)#mpls-vpls V40 service-template VPLS-40`	Bind MPLS VPLS V40 with service template VPLS-40
`RTR6(config_if_vpls)#ac-admin-status up`	Change admin status as UP
`RTR6(config_if_vpls)#exit-if-vpls`	Exit
`RTR6(config)#router bgp 64512`	Configure BGP of as number 64512
`RTR6(config-router)#address-family l2vpn vpls`	Enter into l2vpn VPLS address family
`RTR6(config-router-af)#neighbor 1.1.1.1 activate`	Activate neighbor 1.1.1.1
`RTR6(config-router-af)#exit-address-family`	Exit
`RTR6(config-router)#exit`	Exit
`RTR6(config)#qos enable`	Enable QoS
`RTR6(config)#class-map type queuing que0`	Create class map of type queuing with name que0
`RTR6(config-cmap-que)# match queue 0`	Match for queue 0
`RTR6(config-cmap-que)#class-map type queuing que1`	Create class map of type queuing with name que1
`RTR6(config-cmap-que)#match queue 1`	Match for queue 1
`RTR6(config-cmap-que)#class-map type queuing que2`	Create class map of type queuing with name que2
`RTR6(config-cmap-que)#match queue 2`	Match for queue 2
`RTR6(config-cmap-que)#class-map type queuing que3`	Create class map of type queuing with name que3
`RTR6(config-cmap-que)#match queue 3`	Match for queue 3
`RTR6(config-cmap-que)#class-map type queuing service30`	Create class map of type queuing with name VPLS-30
`RTR6(config-cmap-que)#match service-template VPLS-30`	Match for service template VPLS-30
`RTR6(config-cmap-que)#class-map type queuing service40`	Create class map of type queuing with name VPLS-40
`RTR6(config-cmap-que)#match service-template VPLS-40`	Match for service template VPLS-40
`RTR6(config-cmap-que)#policy-map type queuing queue`	Create policy map with name queue
`RTR6(config-pmap-que)#class type queuing que0`	Add class map que0 to above policy map

RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#class type queuing que1	Add class map que1 to above policy map
RTR6(config-pmap-que)#shape 100 mbps	Shape traffic to 100 mbps
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#class type queuing que2	Add class map que2 to above policy map
RTR6(config-pmap-que)#shape 100 mbps	Shape traffic to 100 mbps
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#class type queuing que3	Add class map que3 to above policy map
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#policy-map type queuing service	Create policy map with name service
RTR6(config-pmap-que)#class type queuing service30	Add class map service30 to above policy map
RTR6(config-pmap-que)#shape 1000 mbps	Shape rate to 1000 mbps
RTR6(config-pmap-c-que)#service-policy queue	Add policy map queue as service-policy
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#class type queuing service40	Add class map service40 to above policymap
RTR6(config-pmap-c-que)#service-policy queue	Add policy map queue as service-policy
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#interface xe13	Configure interface xe13
RTR6(config-if)#service-policy type queuing output service	Attach the policy map service to the interface
RTR6(config-if)#shape rate 3000 mbps	Shape rate traffic to 3000 mbps
RTR6(config-if)#exit	Exit

Validation

RTR6:

```
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 q0                                956.796
 q2                                1032.543
 q4                                1044.794
 q6                                1030.280

RTR6#
RTR6#show running-config qos
```

```
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing service30
 match service-template VPLS-30
!
class-map type queuing service40
 match service-template VPLS-40
!
!
policy-map type queuing queue
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing service30
  service-policy queue
  exit
 class type queuing service40
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output service
!

RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 service30
   que0 (q0)                      510.806
```



```
   que1 (q1)                       514.803
   que2 (q2)                       507.316
   que3 (q3)                       521.820
 service40
   que0 (q0)                       438.860
   que1 (q1)                       530.446
   que2 (q2)                       518.338
   que3 (q3)                       517.863


RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing service30
 match service-template VPLS-30
!
class-map type queuing service40
 match service-template VPLS-40
!
!
policy-map type queuing queue
 class type queuing que0
  exit
 class type queuing que1
  shape 100 mbps
  exit
 class type queuing que2
  shape 100 mbps
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing service30
  shape 1000 mbps
  service-policy queue
  exit
 class type queuing service40
```

```
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output service
 shape rate 3000 mbps
!
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 service30
   que0 (q0)                      415.557
   que1 (q1)                      103.563
   que2 (q2)                      102.592
   que3 (q3)                      412.536
 service40
   que0 (q0)                      438.771
   que1 (q1)                      103.201
   que2 (q2)                      102.954
   que3 (q3)                      515.988
```

L2VPN- VPWS

Figure 18-121 displays a six node topology configured ith end to end connectivity from Router 1 to Router 6. The end to end connectivity is established by configuring OSPF, iBGP and LDP configuration in all the routers. We should be able to ping each device from other device from topology. Configure L2VPN- VPWS services on RTR1 and RTR6 and create Qos configuration on RTR6 and verify service queuing.

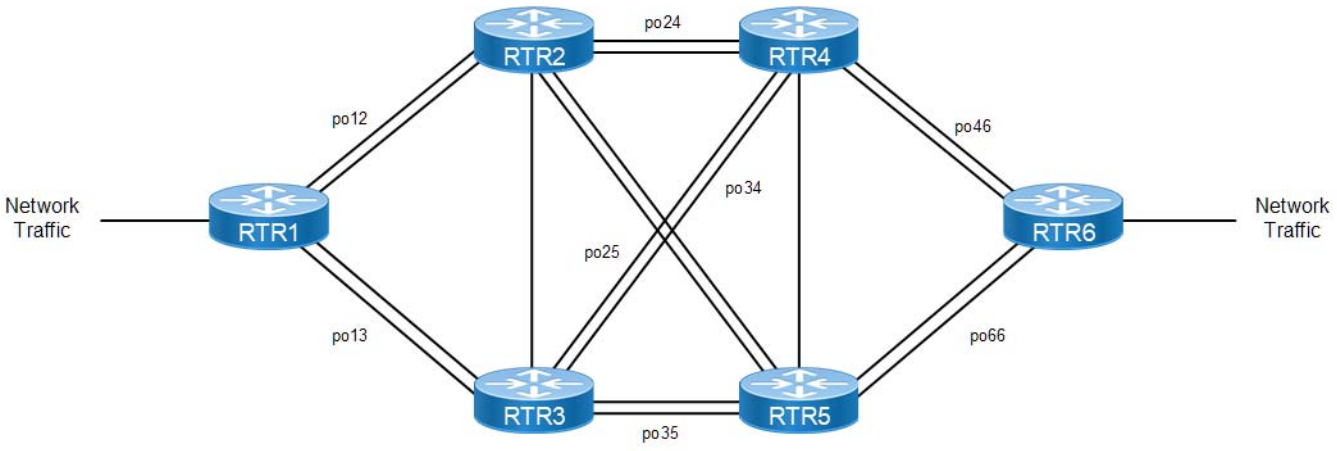


Figure 18-121: Simple Topology

RTR1

`RTR1#configure terminal`	Enter into configuration mode
`RTR1(config)#mpls l2-circuit VPWS10 10 6.6.6.6`	Create MPLS l2 circuit with VPWS10 with ID 10 and end point 6.6.6.6

`RTR1(config)#mpls l2-circuit VPWS20 20 6.6.6.6`	Create MPLS l2 circuit with VPWS20 with ID 20 and end point 6.6.6.6
`RTR1(config)#service-template VPWS-10`	Create service template VPWS-10
`RTR1(config-svc)#match outer-vlan 10`	Match outer vlan 10
`RTR1(config-svc)#rewrite ingress translate 1000 outgoing-tpid dot1.q`	Rewrite ingress translate 1010 with outgoing tpid as dot1q
`RTR1(config-svc)#exit`	Exit
`RTR1(config)#`	
`RTR1(config-svc)#service-template VPWS-20`	Create service template VPWS-20
`RTR1(config-svc)# match outer-vlan 20`	Match outer vlan 20
`RTR1(config-svc)# rewrite ingress translate 1020 outgoing-tpid dot1.q`	Rewrite ingress translate 1020 with outgoing tpid as dot1q
`RTR1(config-svc)#exit`	Exit
`RTR1(config)#interface xe14`	Configure interface xe14
`RTR1(config-if)#switchport`	Configure as layer 2 port
`RTR1(config-if)#load-interval 30`	Configure load interval as 30
`RTR1(config-if)#mpls-l2-circuit VPWS10 service-template VPWS-10`	Attach l2circuit VPWS10 with service template VPWS-10
`RTR1(config-if)#mpls-l2-circuit VPWS20 service-template VPWS-20`	Attach l2circuit VPWS20 with service template VPWS-20
`RTR1(config-if)#exit`	exit

RTR6

`RTR6#configure terminal`	Enter into configuration mode
`RTR6(config)#mpls l2-circuit VPWS10 10 1.1.1.1`	Create MPLS l2 circuit with VPWS10 with ID 10 and end point 1.1.1.1
`RTR6(config)#mpls l2-circuit VPWS20 20 1.1.1.1`	Create MPLS l2 circuit with VPWS20 with ID 20 and end point 1.1.1.1
`RTR6(config)#service-template VPWS-10`	Create service template VPWS-10
`RTR6(config-svc)# match outer-vlan 10`	Match outer vlan 10
`RTR6(config-svc)# rewrite ingress translate 1000 outgoing-tpid dot1.q`	Rewrite ingress translate 1010 with outgoing tpid as dot1q
`RTR6(config-svc)#exit`	Exit
`RTR6(config-svc)#service-template VPWS-20`	Create service template VPWS-20
`RTR6(config-svc)#match outer-vlan 20`	Match outer VLAN 20
`RTR6(config-svc)#rewrite ingress translate 1020 outgoing-tpid dot1.q`	Rewrite ingress translate 1020 with outgoing tpid as dot1q
`RTR6(config-svc)#exit`	Exit
`RTR6(config)#interface xe14`	Configure interface xe14
`RTR6(config-if)#switchport`	Configure as layer 2 port
`RTR6(config-if)#load-interval 30`	Configure load interval as 30
`RTR6(config-if)#mpls-l2-circuit VPWS10 service-template VPWS-10`	Attach l2circuit VPWS10 with service template VPWS-10

`RTR6(config-if)#mpls-l2-circuit VPWS20 service-template VPWS-20`	Attach l2circuit VPWS20 with service template VPWS-20
`RTR6(config-if)#exit`	exit
`RTR6(config)#qos enable`	Enable Qos
`RTR6(config)#class-map type queuing que0`	Create class map of type queuing with name que0
`RTR6(config-cmap-que)# match queue 0`	Match for queue 0
`RTR6(config-cmap-que)#class-map type queuing que1`	Create class map of type queuing with name que1
`RTR6(config-cmap-que)#match queue 1`	Match for queue 1
`RTR6(config-cmap-que)#class-map type queuing que2`	Create class map of type queuing with name que2
`RTR6(config-cmap-que)#match queue 2`	Match for queue 2
`RTR6(config-cmap-que)#class-map type queuing que3`	Create class map of type queuing with name que3
`RTR6(config-cmap-que)#match queue 3`	Match for queue 3
`RTR6(config-cmap-que)#class-map type queuing service10`	Create class map of type queuing with name VPWS-10
`RTR6(config-cmap-que)#match service-template VPWS-10`	Match for service template VPWS-10
`RTR6(config-cmap-que)#class-map type queuing service20`	Create class map of type queuing with name VPWS-20
`RTR6(config-cmap-que)#match service-template VPWS-20`	Match for service template VPWS-20
`RTR6(config-cmap-que)#policy-map type queuing queue`	Create policy map with name queue
`RTR6(config-pmap-que)#class type queuing que0`	Add class map que0 to above policy map
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que1`	Add class map que1 to above policy map
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que2`	Add class map que2 to above policy map
`RTR6(config-pmap-que)#priority level 0`	configure Priority level 0
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que3`	Add class map que3 to above policy map
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#policy-map type queuing service`	Create policy map with name service
`RTR6(config-pmap-que)#class type queuing service10`	Add class map service10 to above policy map
`RTR6(config-pmap-que)#priority level 0`	Change priority level 0
`RTR6(config-pmap-c-que)#service-policy queue`	Add policy map queue as service-policy
`RTR6(config-pmap-c-que)#exit`	Exit

`RTR6(config-pmap-que)#class type queuing service20`	Add class map service20 to above policy map
`RTR6(config-pmap-c-que)#service-policy queue`	Add policy map queue as service-policy
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#interface xe13`	Configure interface xe13
`RTR6(config-if)#service-policy type queuing output service`	Attach the policy map service to the interface
`RTR6(config-if)#shape rate 1000 mbps`	Shape rate traffic to 1000 mbps
`RTR6(config-if)#exit`	Exit

Validation

RTR6:

```
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 q0                                406.907
 q2                                413.234
 q4                                411.703
 q6                                415.307

RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing service10
 match service-template VPWS-10
!
class-map type queuing service20
 match service-template VPWS-20
!
!
policy-map type queuing queue
 class type queuing que0
  exit
```

```
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing service10
  service-policy queue
  exit
 class type queuing service20
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output service
!

RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe0
 q7                                0.178
xe1
 q7                                0.170
xe2
 q7                                0.178
xe3
 q7                                0.186
xe6
 q7                                0.170
xe7
 q7                                0.186
xe8
 q7                                0.170
xe9
 q7                                0.178
xe13
 class-default-q (q0)              207.461
 class-default-q (q2)              207.031
 class-default-q (q4)              207.158
 class-default-q (q6)              197.740
 service10
   que0 (q0)                       107.698
   que1 (q1)                       106.338
   que2 (q2)                       103.133
   que3 (q3)                       105.985
 service20
```



```
   que0 (q0)                      103.376
   que1 (q1)                      102.938
   que2 (q2)                      101.485
   que3 (q3)                      101.537


RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing service10
 match service-template VPWS-10
!
class-map type queuing service20
 match service-template VPWS-20
!
!
policy-map type queuing queue
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  priority level 0
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing service10
  priority level 0
  service-policy queue
  exit
 class type queuing service20
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output service
```

```
 shape rate 1000 mbps
!

RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 class-default-q (q0)              80.431
 class-default-q (q2)              79.903
 class-default-q (q4)              79.780
 class-default-q (q6)              79.605
 service10
   que0 (q0)                       100.546
   que1 (q1)                       105.640
   que2 (q2)                       103.802
   que3 (q3)                       103.724
 service20
   que0 (q0)                       70.014
   que1 (q1)                       69.665
   que2 (q2)                       108.427
   que3 (q3)                       70.090
```

L3VPN- Sub/VLAN interfaces

Figure 18-122 displays a six node topology configured with end to end connectivity from Router 1 to Router 6. The end to end connectivity is established by configuring OSPF, iBGP and LDP configuration in all the routers. We should be able to ping each device from other device from topology. Configure L3VPN with sub interface and VLAN interface configurations on RTR1 and RTR6 and create Qos configuration on RTR6 and verify service queuing.

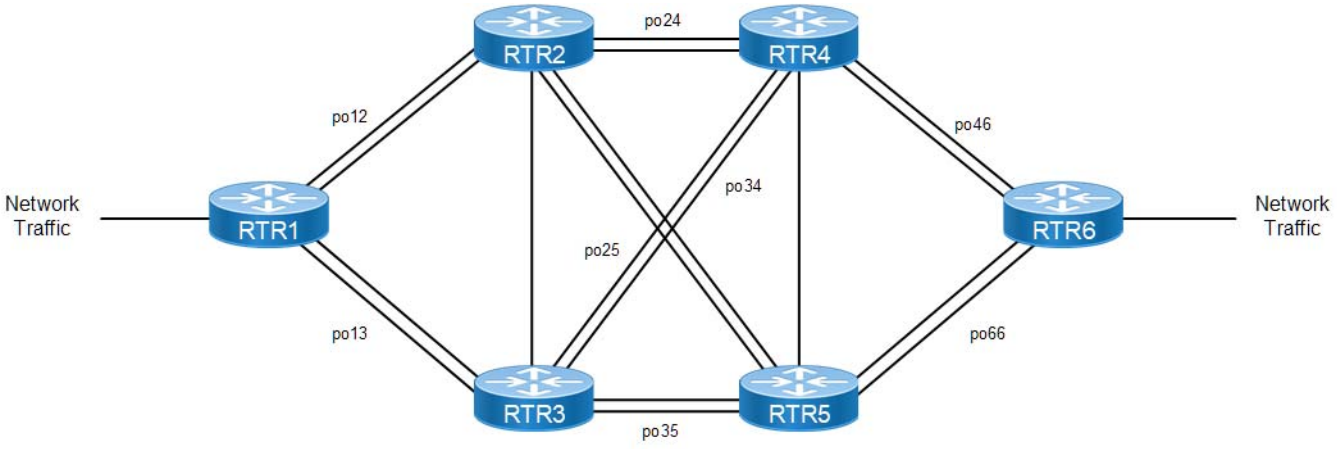


Figure 18-122: Simple Topology

RTR1

`RTR1(config)#ip vrf 3`	Create new vrf with name 3
`RTR1(config-vrf)#rd 2:3`	Create route distinguisher for vrf 3
`RTR1(config-vrf)#route-target both 1:3`	Create route target for vrf 3

`RTR1(config-vrf)#ip vrf 4`	Create new vrf with name 4
`RTR1(config-vrf)#rd 2:4`	Create route distinguisher for vrf 4
`RTR1(config-vrf)#route-target both 1:4`	Create route target for vrf 4
`RTR1(config-vrf)#ip vrf 5`	Create new vrf with name 5
`RTR1(config-vrf)#rd 2:5`	Create route distinguisher for vrf 5
`RTR1(config-vrf)#route-target both 1:5`	Create route target for vrf 5
`RTR1(config-vrf)#ip vrf 6`	Create new vrf with name 6
`RTR1(config-vrf)#rd 2:6`	Create route distinguisher for vrf 6
`RTR1(config-vrf)#route-target both 1:6`	Create route target for vrf 6
`RTR1(config-vrf)#exit`	Exit
`RTR1(config)#interface lo.3`	Configure loopback lo.3
`RTR1(config-if)#ip vrf forwarding 3`	Attach VRF 3 to loopback lo.3 interface
`RTR1(config-if)#interface lo.4`	Configure loopback lo.4
`RTR1(config-if)#ip vrf forwarding 4`	Attach VRF 4 to loopback lo.4 interface
`RTR1(config-if)#interface lo.5`	Configure loopback lo.5
`RTR1(config-if)#ip vrf forwarding 5`	Attach VRF 5 to loopback lo.5 interface
`RTR1(config-if)#interface lo.6`	Configure loopback lo.6
`RTR1(config-if)#ip vrf forwarding 6`	Attach vrf 6 to loopback lo.6 interface
`RTR1(config-if)#exit`	Exit
`RTR1(config)#interface ce52.203`	Create sub interface for ce52 port
`RTR1(config-if)#ip vrf forwarding 3`	Attach vrf 3 to sub int ce52.203
`RTR1(config-if)#ip address 201.203.1.1/24`	Assign ip address 201.203.1.1/24
`RTR1(config-if)#encapsulation dot1q 203`	Encapsulate dot1q VLAN with id 203
`RTR1(config-if)#interface ce52.204`	Create sub interface for ce52 port
`RTR1(config-if)#ip vrf forwarding 4`	Attach vrf 4 to sub int ce52.204
`RTR1(config-if)#ip address 201.204.1.1/24`	Assign ip address 201.204.1.1/24
`RTR1(config-if)#encapsulation dot1q 204`	Encapsulate dot1q VLAN with id 204
`RTR1(config-if)#interface vlan1.205`	Create VLAN interface with id 205
`RTR1(config-if)#ip vrf forwarding 5`	Attach VRF 5 to vlan1.205
`RTR1(config-if)#ip address 201.205.1.1/24`	Assign IP address of 201.205.1.1/24
`RTR1(config-if)#mtu 9216`	Configure MTU of size 9216
`RTR1(config-if)#interface vlan1.206`	Create VLAN interface with id 206
`RTR1(config-if)#ip vrf forwarding 6`	Attach VRF 6 to vlan1.206
`RTR1(config-if)#ip address 201.206.1.1/24`	Assign ip address of 201.206.1.1/24
`RTR1(config-if)#mtu 9216`	Configure MTU of size 9216
`RTR1(config)#router bgp 64512`	Configure router BGP 66512
`RTR1(config-router)#address-family vpnv4 unicast`	Enter into vpnv4 unicast address family
`RTR1(config-router-af)#neighbor 6.6.6.6 activate`	Activate neighbor on vpnv4 unicast
`RTR1(config-router-af)#exit-address-family`	Exit

`RTR1(config-router)#address-family ipv4 vrf 3`	Enter into ipv4 vrf3 address family
`RTR1(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 3
`RTR1(config-router-af)#exit-address-family`	Exit
`RTR1(config-router)#address-family ipv4 vrf 4`	Enter into ipv4 vrf4 address family
`RTR1(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 4
`RTR1(config-router-af)#exit-address-family`	Exit
`RTR1(config-router)#address-family ipv4 vrf 5`	Enter into ipv4 vrf5 address family
`RTR1(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 5
`RTR1(config-router-af)#exit-address-family`	Exit
`RTR1(config-router)#address-family ipv4 vrf 6`	Enter into ipv4 vrf6 address family
`RTR1(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 6
`RTR1(config-router-af)#exit-address-family`	Exit
`RTR1(config-router)#exit`	Exit
`RTR1(config)#interface ce52`	Configure interface ce52
`RTR1(config-if)#load-interval 30`	Configure load interval 30
`RTR1(config-if)#interface ce50`	Configure interface ce50
`RTR1(config-if)#switchport`	Configure port as layer 2 port
`RTR1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR1(config-if)#switchport mode trunk`	Configure interface as trunk port
`RTR1(config-if)#switchport trunk allowed vlan add 205, 206`	Allow only VLANs 205 and 206
`RTR1(config-if)#load-interval 30`	Configure load interval 30

RTR6

`RTR6(config)#ip vrf 3`	Create new vrf with name 3
`RTR6(config-vrf)#rd 1:3`	Create route distinguisher for VRF 3
`RTR6(config-vrf)#route-target both 1:3`	Create route target for VRF 3
`RTR6(config-vrf)#ip vrf 4`	Create new VRF with name 4
`RTR6(config-vrf)#rd 1:4`	Create route distinguisher for VRF 4
`RTR6(config-vrf)#route-target both 1:4`	Create route target for VRF 4
`RTR6(config-vrf)#ip vrf 5`	Create new VRF with name 5
`RTR6(config-vrf)#rd 1:5`	Create route distinguisher for VRF 5
`RTR6(config-vrf)#route-target both 1:5`	Create route target for VRF 5
`RTR6(config-vrf)#ip vrf 6`	Create new VRF with name 6
`RTR6(config-vrf)#rd 1:6`	Create route distinguisher for VRF 6
`RTR6(config-vrf)#route-target both 1:6`	Create route target for VRF 6

RTR6(config-vrf)#exit	Exit
RTR6(config)#interface lo.3	Configure loopback lo.3
RTR6(config-if)#ip vrf forwarding 3	Attach vrf 3 to loopback lo.3 interface
RTR6(config-if)#interface lo.4	Configure loopback lo.4
RTR6(config-if)#ip vrf forwarding 4	Attach vrf 4 to loopback lo.4 interface
RTR6(config-if)#interface lo.5	Configure loopback lo.5
RTR6(config-if)#ip vrf forwarding 5	Attach vrf 5 to loopback lo.5 interface
RTR6(config-if)#interface lo.6	Configure loopback lo.6
RTR6(config-if)#ip vrf forwarding 6	Attach VRF 6 to loopback lo.6 interface
RTR6(config-if)#interface xe13.103	Create sub interface for xe13 port
RTR6(config-if)#ip vrf forwarding 3	Attach VRF 3 to sub int xe13.103
RTR6(config-if)#ip address 101.103.1.1/24	Assign ip address 101.103.1.1/24
RTR6(config-if)#encapsulation dot1q 103	Encapsulate dot1q VLAN with id 103
RTR6(config-if)#interface xe13.104	Create sub interface for xe13.104 port
RTR6(config-if)#ip vrf forwarding 4	Attach VRF 4 to sub int xe13.104
RTR6(config-if)#ip address 101.104.1.1/24	Assign IP address 101.104.1.1/24
RTR6(config-if)#encapsulation dot1q 104	Encapsulate dot1q VLAN with id 104
RTR6(config-if)#interface vlan1.105	Create VLAN interface with id 105
RTR6(config-if)#ip vrf forwarding 5	Attach VRF 5 to vlan1.105
RTR6(config-if)#ip address 101.105.1.1/24	Assign ip address of 101.105.1.1/24
RTR6(config-if)#mtu 9216	Configure MTU of size 9216
RTR6(config-if)#interface vlan1.106	Create VLAN interface with id 106
RTR6(config-if)#ip vrf forwarding 6	Attach VRF 6 to vlan1.106
RTR6(config-if)#ip address 101.106.1.1/24	Assign IP address of 101.106.1.1/24
RTR6(config-if)#mtu 9216	Configure mtu of size 9216
RTR6(config-if)#exit	Exit
RTR6(config)#router bgp 64512	Configure BGP 64512
RTR6(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
RTR6(config-router-af)#neighbor 1.1.1.1 activate	Activate neighbor on vpnv4 unicast
RTR6(config-router-af)#exit-address-family	Exit
RTR6(config-router)#address-family ipv4 vrf 3	Enter into ipv4 vrf3 address family
RTR6(config-router-af)#redistribute connected	Redistribute connected networks into VRF 3
RTR6(config-router-af)#exit-address-family	Exit
RTR6(config-router)#address-family ipv4 vrf 4	Enter into ipv4 vrf4 address family
RTR6(config-router-af)#redistribute connected	Redistribute connected networks into vrf 4
RTR6(config-router-af)#exit-address-family	Exit

`RTR6(config-router)#address-family ipv4 vrf 5`	Enter into ipv4 vrf5 address family
`RTR6(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 5
`RTR6(config-router-af)#exit-address-family`	Exit
`RTR6(config-router)#address-family ipv4 vrf 6`	Enter into ipv4 vrf6 address family
`RTR6(config-router-af)#redistribute connected`	Redistribute connected networks into vrf 6
`RTR6(config-router-af)#exit-address-family`	Exit
`RTR6(config-router)#exit`	Exit
`RTR6(config)#interface xe13`	Configure interface xe13
`RTR6(config-if)#load-interval 30`	Configure load interval 30
`RTR6(config-if)#interface xe14`	Configure interface xe14
`RTR6(config-if)#switchport`	Configure port as layer 2 port
`RTR6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR6(config-if)#switchport mode trunk`	Configure interface as trunk port
`RTR6(config-if)#switchport trunk allowed vlan add 105,106`	Allow only vlans105 and 106
`RTR6(config-if)#load-interval 30`	Configure load interval 30
`RTR6(config-if)#exit`	Exit

Validation

Validation for sub interfaces

RTR6:

```
RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing xe13.103
 match interface xe13.103
!
class-map type queuing xe13.104
 match interface xe13.104
```

```
!
!
policy-map type queuing queuePolicy
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing xe13.103
  service-policy queuePolicy
  exit
 class type queuing xe13.104
  service-policy queuePolicy
  exit
interface xe13
 service-policy type queuing output service
!

RTR6#
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 xe13.103
   que0 (q0)                      499.345
   que1 (q1)                      507.020
   que2 (q2)                      510.231
   que3 (q3)                      503.312
 xe13.104
   que0 (q0)                      502.730
   que1 (q1)                      497.862
   que2 (q2)                      508.641
   que3 (q3)                      489.681
RTR6#

RTR6# show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
```

```
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing xe13.103
 match interface xe13.103
!
class-map type queuing xe13.104
 match interface xe13.104
!
!
!
policy-map type queuing queuePolicy
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing service
 class type queuing xe13.103
  service-policy queuePolicy
  exit
 class type queuing xe13.104
  priority level 0
  service-policy queuePolicy
  exit
!
interface xe13
 service-policy type queuing output service
 shape rate 4000 mbps
!
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 xe13.103
   que0 (q0)                      82.403
   que1 (q1)                      83.355
   que2 (q2)                      82.881
   que3 (q3)                      83.354
 xe13.104
   que0 (q0)                      498.243
   que1 (q1)                      502.950
```



```
   que2 (q2)                       510.054
   que3 (q3)                       494.921

Validation for vlan interfaces
RTR6:
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 q0                              1988.796
 q1                              1976.734
 q5                              1997.010
 q6                              2022.276
 q7                              0.012

RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing vlan1.105
 match interface vlan1.105
!
class-map type queuing vlan1.106
 match interface vlan1.106
!
!
policy-map type queuing queuePolicy
 class type queuing que0
  shape 100 mbps
  exit
 class type queuing que1
  exit
 class type queuing que2
  shape 150 mbps
  exit
 class type queuing que3
  exit
!
```

```
policy-map type queuing service
 class type queuing vlan1.105
  service-policy queuePolicy
  exit
 class type queuing vlan1.106
  wfq-queue weight 4
  service-policy queuePolicy
  exit
!
interface xe13
 service-policy type queuing output service
 shape rate 6000 mbps
!
RTR6#  show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 vlan1.105
   que0 (q0)                      99.882
   que1 (q1)                      508.907
   que2 (q2)                      150.103
   que3 (q3)                      505.349
 vlan1.106
   que0 (q0)                      100.148
   que1 (q1)                      505.652
   que2 (q2)                      149.896
   que3 (q3)                      501.783
```

Provider Bridge

Figure 18-123 displays a six node topology configured with end to end connectivity from Router 1 to Router 6. The end to end connectivity is established by configuring OSPF, iBGP and LDP configuration in all the routers. We should be able to ping each device from other device from topology.

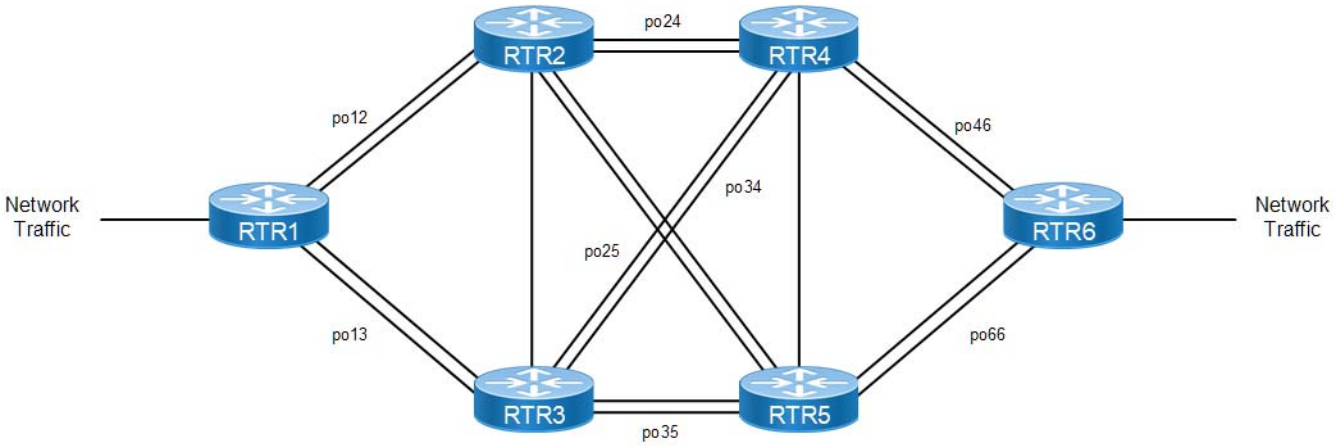


Figure 18-123: Simple Topology

RTR1

`RTR1#configure terminal`	Enter into configure terminal mode
`RTR1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge 1 protocol as provider RSTP edge
`RTR1(config)#vlan database`	Configure VLAN database
`RTR1(config-vlan)#vlan 201-300 type customer bridge 1 state enable`	Configure customer VLANs from 201-300
`RTR1(config-vlan)#vlan 301-400 type service point-point bridge 1 state enable`	Configure service VLANs from 301-400
`RTR1(config-vlan)#cvlan registration table map1 bridge 1`	Create cvlan registration table
`RTR1(config-cvlan-registration)#cvlan 201 svlan 301`	Map 201 cvlan to 301 svlan
`RTR1(config-cvlan-registration)#cvlan 202 svlan 302`	Map 202 cvlan to 302 svlan
`RTR1(config-cvlan-registration)#cvlan 203 svlan 303`	Map 203 cvlan to 303 svlan
`RTR1(config-cvlan-registration)#cvlan 204 svlan 304`	Map 204 cvlan to 304 svlan
`RTR1(config-cvlan-registration)#cvlan 205 svlan 305`	Map 205 cvlan to 305 svlan
`RTR1(config-cvlan-registration)#interface po12`	Configure interface po12
`RTR1(config-if)#switchport`	Configure as layer 2 port
`RTR1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR1(config-if)#switchport mode provider-network`	Configure switchport mode as provider network
`RTR1(config-if)#switchport provider-network allowed vlan add 301-400`	Configure allowed VLAN from 301-400
`RTR1(config-if)#load-interval 30`	Configure load interval 30
`RTR1(config-if)#interface po13`	Configure interface po13
`RTR1(config-if)#switchport`	Configure as layer 2 port
`RTR1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR1(config-if)#switchport mode provider-network`	Configure switchport mode as provider network
`RTR1(config-if)#switchport provider-network allowed vlan add 301-400`	Configure allowed vlan from 301-400
`RTR1(config-if)#load-interval 30`	Configure load interval 30
`RTR1(config-if)#interface xe1`	Configure xe1
`RTR1(config-if)#channel-group 12 mode active`	Add xe1 to po12
`RTR1(config-if)#interface xe2`	Configure xe2
`RTR1(config-if)#channel-group 12 mode active`	Add xe2 to po12
`RTR1(config-if)#interface xe3`	Configure xe3

`RTR1(config-if)#channel-group 13 mode active`	Add xe3 to po13
`RTR1(config-if)#interface xe4`	Configure xe4
`RTR1(config-if)#channel-group 13 mode active`	Add xe4 to po13
`RTR1(config-if)#interface xe15`	Configure interface xe15
`RTR1(config-if)#switchport`	Configure as layer 2 port
`RTR1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR1(config-if)#switchport mode customer-edge trunk`	Configure switchport mode as customer edge trunk
`RTR1(config-if)#switchport customer-edge trunk allowed vlan add 201-300`	Configure allowed vlan from 201-300
`RTR1(config-if)#switchport customer-edge vlan registration map1`	Attach VLAN registration table map 1 to xe15
`RTR1(config-if)#load-interval 30`	Configure load interval 30
`RTR1(config-if)#exit`	Exit

RTR2

`RTR2#configure terminal`	Configure terminal
`RTR2(config)#bridge 1 protocol provider-rstp`	Configure bridge 1 protocol as provider rstp edge
`RTR2(config)#vlan database`	VLAN database
`RTR2(config-vlan)#vlan 301-400 type service point-point bridge 1 state enable`	Configure service vlans from 301-400
`RTR2(config-vlan)#interface po12`	Configure interface po12
`RTR2(config-if)#switchport`	Configure as layer 2 port
`RTR2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR2(config-if)#switchport mode provider-network`	Configure switchport mode as provider network
`RTR2(config-if)#switchport provider-network allowed vlan add 301-400`	Configure allowed vlan from 301-400
`RTR2(config-if)#load-interval 30`	Configure load interval 30
`RTR2(config-if)#interface po24`	Configure interface po24
`RTR2(config-if)#switchport`	Configure as layer 2 port
`RTR2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR2(config-if)#switchport mode provider-network`	Configure switchport mode as provider network
`RTR2(config-if)#switchport provider-network allowed vlan add 301-400`	Configure allowed vlan from 301-400
`RTR2(config-if)#load-interval 30`	Configure load interval 30
`RTR2(config-if)#interface po25`	Configure interface po25
`RTR2(config-if)#switchport`	Configure as layer 2 port
`RTR2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR2(config-if)#switchport mode provider-network`	Configure switchport mode as provider network

RTR2(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR2(config-if)#load-interval 30	Configure load interval 30
RTR2(config-if)#interface xe1	Configure xe1
RTR2(config-if)#channel-group 12 mode active	Add xe1 to po12
RTR2(config-if)#interface xe2	Configure xe2
RTR2(config-if)#channel-group 12 mode active	Add xe2 to po12
RTR2(config-if)#interface xe8	Configure xe8
RTR2(config-if)#channel-group 25 mode active	Add xe8 to po25
RTR2(config-if)#interface xe9	Configure xe9
RTR2(config-if)#channel-group 25 mode active	Add xe9 to po25
RTR2(config-if)#interface xe14	Configure xe14
RTR2(config-if)#channel-group 24 mode active	Add xe14 to po24
RTR2(config-if)#interface xe15	Configure xe15
RTR2(config-if)#channel-group 24 mode active	Add xe15 to po24
RTR2(config)#exit	Exit

RTR3

RTR3#config term	Configure terminal
RTR3(config)#bridge 1 protocol provider-rstp	Configure bridge 1 protocol as provider rstp edge
RTR3(config)#vlan database	Configure VLAN database
RTR3(config-vlan)#vlan 301-400 type service point-point bridge 1 state enable	Configure service VLANS from 301-400
RTR3(config-vlan)#interface po13	Configure interface po13
RTR3(config-if)# switchport	Configure as layer 2 port
RTR3(config-if)# bridge-group 1	Configure interface in bridge group 1
RTR3(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR3(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR3(config-if)#load-interval 30	Configure load interval 30
RTR3(config-if)#interface po34	Configure interface po34
RTR3(config-if)#switchport	Configure as layer 2 port
RTR3(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR3(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR3(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400

RTR3(config-if)#load-interval 30	Configure load interval 30
RTR3(config-if)#interface po35	Configure interface po35
RTR3(config-if)#switchport	Configure as layer 2 port
RTR3(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR3(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR3(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR3(config-if)#load-interval 30	Configure load interval 30
RTR3(config-if)#interface xe3	Configure xe3
RTR3(config-if)#channel-group 13 mode active	Add xe3 to po13
RTR3(config-if)#interface xe4	Configure xe4
RTR3(config-if)# channel-group 13 mode active	Add xe4 to po13
RTR3(config-if)#interface xe7	Configure xe7
RTR3(config-if)#channel-group 34 mode active	Add xe7 to po34
RTR3(config-if)#interface xe8	Configure xe8
RTR3(config-if)#channel-group 34 mode active	Add xe8 to po34
RTR3(config-if)#interface xe14	Configure xe14
RTR3(config-if)#channel-group 35 mode active	Add xe14 to po35
RTR3(config-if)#interface xe15	Configure xe15
RTR3(config-if)#channel-group 35 mode active	Add xe15 to po35
RTR3(config-if)#exit	Exit

RTR4

RTR4#config term	Configure terminal
RTR4(config)#bridge 1 protocol provider-rstp	Configure bridge 1 protocol as provider rstp edge
RTR4(config)#vlan database	Configure vlan database
RTR4(config-vlan)#vlan 301-400 type service point-point bridge 1 state enable	Configure service vlans from 301-400
RTR4(config-vlan)#interface po24	Configure interface po24
RTR4(config-if)#switchport	Configure as layer 2 port
RTR4(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR4(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR4(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed VLAN from 301-400
RTR4(config-if)#load-interval 30	Configure load interval 30
RTR4(config-if)#interface po34	Configure interface po34

RTR4(config-if)#switchport	Configure as layer 2 port
RTR4(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR4(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR4(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR4(config-if)#load-interval 30	Configure load interval 30
RTR4(config-if)#interface po46	Configure interface po46
RTR4(config-if)#switchport	Configure as layer 2 port
RTR4(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR4(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR4(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR4(config-if)#load-interval 30	Configure load interval 30
RTR4(config-if)#interface xe0	Configure xe0
RTR4(config-if)#channel-group 46 mode active	Add xe0 to po46
RTR4(config-if)#interface xe1	Configure xe1
RTR4(config-if)#channel-group 46 mode active	Add xe1 to po46
RTR4(config-if)#interface xe2	Configure xe2
RTR4(config-if)#channel-group 46 mode active	Add xe2 to po46
RTR4(config-if)#interface xe3	Configure xe3
RTR4(config-if)#channel-group 46 mode active	Add xe3 to po46
RTR4(config-if)#interface xe7	Configure xe7
RTR4(config-if)#channel-group 34 mode active	Add xe7 to po34
RTR4(config-if)#interface xe8	Configure xe8
RTR4(config-if)#channel-group 34 mode active	Add xe8 to po34
RTR4(config-if)#interface xe14	Configure xe14
RTR4(config-if)#channel-group 24 mode active	Add xe14 to po24
RTR4(config-if)#interface xe15	Configure xe15
RTR4(config-if)#channel-group 24 mode active	Add xe15 to po24
RTR4(config-if)#end	End

RTR5

RTR5#config term	Configure terminal
RTR5(config)#bridge 1 protocol provider-rstp	Configure bridge 1 protocol as provider rstp edge

RTR5(config)#vlan database	Configure vlan database
RTR5(config-vlan)#vlan 301-305 type service point-point bridge 1 state enable	Configure service vlans from 301-305
RTR5(config-vlan)#interface po25	Configure interface po25
RTR5(config-if)#switchport	Configure as layer 2 port
RTR5(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR5(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR5(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR5(config-if)#load-interval 30	Configure load interval 30
RTR5(config-if)#interface po35	Configure interface po35
RTR5(config-if)#switchport	Configure as layer 2 port
RTR5(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR5(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR5(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR5(config-if)#load-interval 30	Configure load interval 30
RTR5(config-if)#interface po56	Configure interface po56
RTR5(config-if)#switchport	Configure as layer 2 port
RTR5(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR5(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR5(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR5(config-if)#load-interval 30	Configure load interval 30
RTR5(config-if)#interface xe2	Configure xe2
RTR5(config-if)#channel-group 25 mode active	Add xe2 to po25
RTR5(config-if)#interface xe3	Configure xe3
RTR5(config-if)#channel-group 25 mode active	Add xe3 to po25
RTR5(config-if)#interface xe6	Configure xe6
RTR5(config-if)#channel-group 56 mode active	Add xe6 to po56
RTR5(config-if)#interface xe7	Configure xe7
RTR5(config-if)#channel-group 56 mode active	Add xe7 to po56
RTR5(config-if)#interface xe8	Configure xe8
RTR5(config-if)#channel-group 56 mode active	Add xe8 to po56
RTR5(config-if)#interface xe9	Configure xe9
RTR5(config-if)#channel-group 56 mode active	Add xe9 to po56

RTR5(config-if)#interface xe14	Configure xe14
RTR5(config-if)#channel-group 35 mode active	Add xe14 to po35
RTR5(config-if)#interface xe15	Configure xe15
RTR5(config-if)#channel-group 35 mode active	Add xe15 to po35
RTR5(config-if)#end	End

RTR6

RTR6#config terminal	Configure terminal
RTR6(config)#bridge 1 protocol provider-rstp edge	Configure bridge 1 protocol as provider rstp edge
RTR6(config)#vlan database	Configure vlan database
RTR6(config-vlan)#vlan 201-300 type customer bridge 1 state enable	Configure customer VLANS from 201-300
RTR6(config-vlan)#vlan 301-400 type service point-point bridge 1 state enable	Configure service VLANs from 301-400
RTR6(config-vlan)#cvlan registration table map1 bridge 1	Create cvlan registration table
RTR6(config-cvlan-registration)#cvlan 201 svlan 301	Map 201 cvlan to 301 svlan
RTR6(config-cvlan-registration)#cvlan 202 svlan 302	Map 202 cvlan to 302 svlan
RTR6(config-cvlan-registration)#cvlan 203 svlan 303	Map 203 cvlan to 303 svlan
RTR6(config-cvlan-registration)#cvlan 204 svlan 304	Map 204 cvlan to 304 svlan
RTR6(config-cvlan-registration)#cvlan 205 svlan 305	Map 205 cvlan to 305 svlan
RTR6(config-cvlan-registration)#interface po46	Configure interface po46
RTR6(config-if)#switchport	Configure as layer 2 port
RTR6(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR6(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR6(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR6(config-if)#load-interval 30	Configure load interval 30
RTR6(config-if)#interface po56	Configure interface po56
RTR6(config-if)#switchport	Configure as layer 2 port
RTR6(config-if)#bridge-group 1	Configure interface in bridge group 1
RTR6(config-if)#switchport mode provider-network	Configure switchport mode as provider network
RTR6(config-if)#switchport provider-network allowed vlan add 301-400	Configure allowed vlan from 301-400
RTR6(config-if)#load-interval 30	Configure load interval 30

`RTR6(config-if)#interface xe0`	Configure xe0
`RTR6(config-if)#channel-group 46 mode active`	Add xe0 to po46
`RTR6(config-if)#interface xe1`	Configure xe1
`RTR6(config-if)#channel-group 46 mode active`	Add xe1 to po46
`RTR6(config-if)#interface xe2`	Configure xe2
`RTR6(config-if)#channel-group 46 mode active`	Add xe2 to po46
`RTR6(config-if)#interface xe3`	Configure xe3
`RTR6(config-if)#channel-group 46 mode active`	Add xe3 to po46
`RTR6(config-if)#interface xe6`	Configure xe6
`RTR6(config-if)#channel-group 56 mode active`	Add xe6 to po56
`RTR6(config-if)#interface xe7`	Configure xe7
`RTR6(config-if)#channel-group 56 mode active`	Add xe7 to po56
`RTR6(config-if)#interface xe8`	Configure xe8
`RTR6(config-if)#channel-group 56 mode active`	Add xe8 to po56
`RTR6(config-if)#interface xe9`	Configure xe9
`RTR6(config-if)#channel-group 56 mode active`	Add xe9 to po56
`RTR6(config-if)#interface xe15`	Configure interface xe15
`RTR6(config-if)#switchport`	Configure as layer 2 port
`RTR6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`RTR6(config-if)#switchport mode customer-edge trunk`	Configure switchport mode as customer edge trunk
`RTR6(config-if)#switchport customer-edge trunk allowed vlan add 201-300`	Configure allowed vlan from 201-300
`RTR6(config-if)#switchport customer-edge vlan registration map1`	Attach vlan registration table map 1 to xe15
`RTR6(config-if)#load-interval 30`	Configure load interval 30
`RTR6(config)#class-map type queuing que0`	Create Class map type queuing que0
`RTR6(config-cmap-que)#match queue 0`	Match for queue 0
`RTR6(config-cmap-que)#class-map type queuing que1`	Create Class map type queuing que0
`RTR6(config-cmap-que)#match queue 1`	Match for queue 1
`RTR6(config-cmap-que)#class-map type queuing que2`	Create Class map type queuing que1
`RTR6(config-cmap-que)#match queue 2`	Match for queue 2
`RTR6(config-cmap-que)#class-map type queuing que3`	Create Class map type queuing que2
`RTR6(config-cmap-que)#match queue 3`	Match for queue 3

`RTR6(config-cmap-que)#class-map type queuing vlan201`	Create class map type queuing vlan201
`RTR6(config-cmap-que)#match vlan 201`	Match for VLAN 201
`RTR6(config-cmap-que)#class-map type queuing vlan202`	Create class map type queuing vlan202
`RTR6(config-cmap-que)#match vlan 202`	Match for VLAN 202
`RTR6(config-cmap-que)#class-map type queuing vlan203`	Create class map type queuing vlan203
`RTR6(config-cmap-que)#match vlan 203`	Match for VLAN 203
`RTR6(config-cmap-que)#class-map type queuing vlan204`	Create class map type queuing vlan204
`RTR6(config-cmap-que)#match vlan 204`	Match for VLAN 204
`RTR6(config-cmap-que)#policy-map type queuing queue`	Create policy map of type queuing with name queue
`RTR6(config-pmap-que)#class type queuing que0`	Attach class map que0
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que1`	Attach class map que1
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que2`	Attach class map que2
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing que3`	Attach class map que3
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#policy-map type queuing vlan`	Create policy map of type queuing with name vlan
`RTR6(config-pmap-que)#class type queuing vlan201`	Attach class map vlan201
`RTR6(config-pmap-c-que)#service-policy queue`	Attach service policy queue
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing vlan202`	Attach class map vlan202
`RTR6(config-pmap-c-que)#shape 100 mbps`	Shape traffic to 100 mbps
`RTR6(config-pmap-c-que)#service-policy queue`	Attach service policy queue
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing vlan203`	Attach class map vlan203
`RTR6(config-pmap-c-que)#service-policy queue`	Attach service policy queue
`RTR6(config-pmap-c-que)#exit`	Exit
`RTR6(config-pmap-que)#class type queuing vlan204`	Attach class map vlan204

RTR6(config-pmap-c-que)#service-policy queue	Attach service policy queue
RTR6(config-pmap-c-que)#exit	Exit
RTR6(config-pmap-que)#interface xe13	Configure interface xe13
RTR6(config-if)#service-policy type queuing output vlan	Attach service policy vlan to interface xe13
RTR6(config-if)#shape rate 1000 mbps	Shape rate 1000 mbps
RTR6(config-if)#exit	Exit

Validation

RTR6:

```
RTR6#show running-config qos
qos enable
!
RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 q0                                407.399
 q2                                415.419
 q4                                398.478
 q6                                411.140


RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing vlan201
 match vlan 201
!
class-map type queuing vlan202
 match vlan 202
!
class-map type queuing vlan203
```

```
 match vlan 203
!
class-map type queuing vlan204
 match vlan 204
!
!
policy-map type queuing queue
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing vlan
 class type queuing vlan201
  service-policy queue
  exit
 class type queuing vlan202
  service-policy queue
  exit
 class type queuing vlan203
  service-policy queue
  exit
 class type queuing vlan204
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output vlan
!

RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 vlan201
   que0 (q0)                      98.957
   que1 (q1)                      106.502
   que2 (q2)                      103.779
   que3 (q3)                      100.639
 vlan202
   que0 (q0)                      102.953
   que1 (q1)                      96.453
   que2 (q2)                      103.694
   que3 (q3)                      100.486
 vlan203
```

```
   que0 (q0)                      100.919
   que1 (q1)                      95.551
   que2 (q2)                      103.445
   que3 (q3)                      105.183
 vlan204
   que0 (q0)                      101.593
   que1 (q1)                      101.609
   que2 (q2)                      102.030
   que3 (q3)                      102.992

RTR6#show running-config qos
qos enable
!
class-map type queuing que0
 match queue 0
!
class-map type queuing que1
 match queue 1
!
class-map type queuing que2
 match queue 2
!
class-map type queuing que3
 match queue 3
!
class-map type queuing vlan201
 match vlan 201
!
class-map type queuing vlan202
 match vlan 202
!
class-map type queuing vlan203
 match vlan 203
!
class-map type queuing vlan204
 match vlan 204
!
!
policy-map type queuing queue
 class type queuing que0
  exit
 class type queuing que1
  exit
 class type queuing que2
  exit
 class type queuing que3
  exit
!
policy-map type queuing vlan
 class type queuing vlan201
```

```
  service-policy queue
  exit
 class type queuing vlan202
  shape 100 mbps
  service-policy queue
  exit
 class type queuing vlan203
  service-policy queue
  exit
 class type queuing vlan204
  service-policy queue
  exit
!
interface xe13
 service-policy type queuing output vlan
 shape rate 1000 mbps
!

RTR6#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe13
 vlan201
   que0 (q0)                      75.224
   que1 (q1)                      74.814
   que2 (q2)                      75.476
   que3 (q3)                      75.298
 vlan202
   que0 (q0)                      25.327
   que1 (q1)                      25.068
   que2 (q2)                      24.684
   que3 (q3)                      25.379
 vlan203
   que0 (q0)                      75.943
   que1 (q1)                      75.859
   que2 (q2)                      75.492
   que3 (q3)                      75.115
 vlan204
   que0 (q0)                      75.513
   que1 (q1)                      75.295
   que2 (q2)                      75.907
   que3 (q3)                      76.048
```

CHAPTER 19 Queue Compensation

The size of packets transmitted may vary from the size of packets queued in ingress and egress queues. Contributing factors are:

1. Ethernet Overhead

   Fixed size, typically 20-bytes

2. Internal DRAM CRC

   Fixed size, 2-byte CRC

3. Packet editing resulting from Packet Processing

   Size may vary per queue or per packet

   Network header termination (i.e., Layer-3 link layer termination from routing, MPLS/IP tunnel termination, VLAN Tag removal)

   Network header encapsulation (i.e., Layer-3 link layer encapsulation, MPLS/IP tunnel initiation, Vlan tag addition)

These bytes need to be adjusted to achieve the proper egress rate. Hence, compensation is used to adjust this byte difference in order to achieve the expected egress rate.

The default compensation for all queues is set to -22 internally (Ethernet overhead + internal CRC). This is as per the internal headers in the packet pipeline.

When an attachment-circuit is created on a port the compensation is updated as shown in Table 19-82.

Table 19-82: Compensation updates

AC ingress operation	Compensation
POP	-38
NONE/Translate	-42 (defaults)
PUSH	-46

Note: It is the operator's responsibility to update the compensation if required per application.

The user can configure compensation on the class-maps matching services for service queues, and class-map for “class-default-q” for port queues.

CLI: `compensation <-64-64>`

For example:

```
class-map type queuing data
 match queue 0
!
class-map type queuing service1
 match service-template ETH-2016
!
class-map type queuing service2
 match service-template ETH-2017
!
class-map type queuing signal
 match queue 3
```

```
!
class-map type queuing voice
 match queue 1
!
policy-map type queuing configPolicy1
 class type queuing class-default-q
  exit
 class type queuing data
  exit
 class type queuing signal
  exit
 class type queuing voice
  exit
!
policy-map type queuing customer1
 class type queuing service1
  compensation -20
  service-policy configPolicy1
 class type queuing class-default-q
  compensation -20
  exit
!
interface xe11
 service-policy type queuing output customer1
```

CHAPTER 20 Hierarchical Traffic Policing

Basic traffic policing is explained in Chapter 3, *Traffic Policing*, which covers single-level policing. The Qumran device support two level hierarchical policing in addition to single level traffic policing (Hierarchical policing is also in compliance with RFC 2697 and RFC 4115).

Hierarchical policing ensures traffic policing in two levels in serial mode. Traffic is policed with a “child policer” configuration first, and then policed at a second level, the “parent policer” configuration. Thus, traffic is treated with two levels of policing.

Hierarchical policing will be useful when traffic to be policed per service and additionally to be policed per customers of that particular service. Hierarchical policing is useful when multiple streams (such as voice, data) of customer traffic to be policed and additionally, traffic to be policed per customer. Configuration considerations for hierarchical policing are same as mentioned in Chapter 3, *Traffic Policing*.

Configuring Hierarchical Traffic Policing

Command to configure policing on a class remains same as explained in Chapter 3, *Traffic Policing*.

In addition to the commands explained in Chapter 1, *Quality of Service (QoS)* and Chapter 2, *Configuring a QoS Policy-map*, binding a child policy-map to a parent class is done using the following command:

```
service-policy NAME
```

Notice that `NAME` represents the name of the child qos policy-map. This command is configurable on the class mode as shown in the example below:

```
(config)#policy-map Pmap-Parent-1
(config-pmap-qos)#class Cmap-Parent-1
(config-pmap-c-qos)#service-policy Pmap-Child-1
(config-pmap-c-qos)#exit
```

An example of creating parent and child class-maps and policy-maps, and configuring them for hierarchical policing is shown below:

Note: the qos-policer TCAM group must be enabled before binding a parent policy-map to an interface. For more information about the hardware filter groups, refer to the *Hardware-profile Filters* and the *Show Hardware-profile Filters* sections in the *Qumran Command Reference Guide.*

In the following example, traffic streams on VLAN ID 10, where one stream with CoS value 1 and another stream with CoS value 2 (received on interface xe1) are policed to a total of 40 mbps with 10 mbps of traffic being marked green for stream1 at 20 mbps, and traffic marked green for stream2. The remaining 10 mbps of traffic from stream1 and stream2 is marked yellow. Any remaining traffic will be dropped at ingress.

```
(config)#qos enable
(config)#class-map CUST-10
(config-cmap-qos)#match vlan 10
(config-cmap-qos)#exit
(config)#class-map CUST-10-C1
(config-cmap-qos)#match cos 1
(config-cmap-qos)#exit
(config)#class-map CUST-10-C2
(config-cmap-qos)#match cos 2
(config-cmap-qos)#exit
(config)#policy-map PC-CUST-10
(config-pmap-qos)#class CUST-10-C1
```

```
(config-pmap-c-qos)#police cir 10 mbps eir 30 mbps
(config-pmap-c-qos)#exit
(config-pmap-qos)#class CUST-10-C2
(config-pmap-c-qos)#police cir 20 mbps eir 20 mbps
(config-pmap-c-qos)#exit
(config-pmap-qos)#class class-default
(config-pmap-c-qos)#police cir 10 mbps eir 30 mbps
(config-pmap-c-qos)#exit
(config-pmap-qos)#exit
(config)#policy-map P-CUST-10
(config-pmap-qos)#class CUST-10
(config-pmap-c-qos)#police cir 40 mbps
(config-pmap-c-qos)#service-policy PC-CUST-10
(config-pmap-c-qos)#exit
(config-pmap-qos)#exit
(config)#hardware-profile filter qos-policer enable
(config)#interface xe1
(config-if)#service-policy type qos input P-CUST-10
(config-if)#exit
```

Configuring Hierarchical Policing per Attachment Circuit

In this section, a configuration example is provided for the use-case of configuring traffic policing per attachment circuit with additional traffic policing based on the class of traffic. The configuration helps in providing overall traffic policing per attachment circuit and additionally ensures that different classes of traffic are policed. Total CIR configurations for child classes must be ensured to match the police rate of parent and EIR values for child can be configured to take the available bandwidth when one or more child traffic is not received at any point in time.

Topology

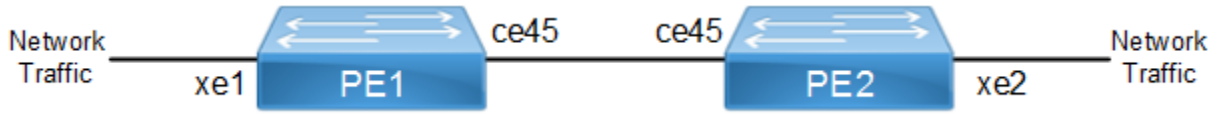


Figure 20-124: Topology for per-AC hierarchical policing

PE1

`PE1#configure terminal`	Enter configure terminal mode
`PE1(config)#hardware-profile filter ingress-ipv6 enable`	Enabling Ingress IPv6 group for IPv6 feature support
`PE1(config)#hardware-profile filter qos-policer enable`	Enabling Ingress extended QOS group for hierarchical policer
`PE1(config)#qos enable`	Enabling QoS
`PE1(config)#qos statistics`	Enabling Qos statistics
`PE1(config)#mpls l2-circuit VPWS-VLAN-200 2000200 21.21.21.21`	Create an instance of an MPLS layer 2 virtual circuit

PE1(config)#mpls l2-circuit VPWS-VLAN-300 2000300 21.21.21.21	Create an instance of an MPLS layer 2 virtual circuit
PE1(config)#mpls lsp-model uniform	Configure the MPLS LSP model as Uniform.
PE1(config)#service-template VPWS-Vlan200-Service	Enabling Service Template
PE1(config-svc)#match outer-vlan 200	Match outer vlan 200
PE1(config-svc)#rewrite ingress translate 100 outgoing-tpid dot1.q	Enabling command to configure a match VLAN action for a service template
PE1(config-svc)#exit	Exit mode
PE1(config)#service-template VPWS-Vlan300-Service	Enabling Service Template
PE1(config-svc)#match outer-vlan 300	Match outer vlan 300<null>
PE1(config-svc)#rewrite ingress translate 4000 outgoing-tpid dot1.q	Enabling command to configure a match VLAN action for a service template
PE1(config-svc)#exit	Exit mode
PE1(config)#class-map c0	Enter Class-map mode
PE1(config-cmap-qos)#match cos 0	Matching cos value inside class map
PE1(config-cmap-qos)#exit	Exit mode
PE1(config)#class-map c1	Enter Class-map mode
PE1(config-cmap-qos)#match cos 1	Matching cos value inside class map
PE1(config-cmap-qos)#exit	Exit mode
PE1(config)#class-map c2	Enter Class-map mode
PE1(config-cmap-qos)#match cos 2	Matching cos value inside class map
PE1(config-cmap-qos)# exit	Exit mode
PE1(config)#class-map c3	Enter Class-map mode
PE1(config-cmap-qos)#match cos 3	Matching cos value inside class map
PE1(config)#class-map cp1	Enter Class-map mode
PE1(config-cmap-qos)#match vlan 200	Matching vlan inside class map
PE1(config-cmap-qos)#exit	Exit mode
PE1(config)#class-map cp2	Enter Class-map mode
PE1(config-cmap-qos)#match vlan 300	Matching vlan inside class map
PE1(config-cmap-qos)#exit	Exit mode
PE1(config)#policy-map child	Enter policy-map mode
PE1(config-pmap-qos)#class c0	Assign Class c0 to Policy-map child
PE1(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#class c1	Assign Class c1 to Policy-map child
PE1(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#class c2	Assign Class c2 to Policy-map child
PE1(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps

PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#class c3	Assign Class c3 to Policy-map child
PE1(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#policy-map parent	Enter policy-map mode
PE1(config-pmap-qos)#class cp1	Assign Class cp1 to Policy-map parent
PE1(config-pmap-c-qos)#police cir 200 mbps	Police packets @ Committed information rate 200 mbps
PE1(config-pmap-c-qos)#service-policy child	Attaching child policy to Parent
PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#class cp2	Assign Class cp2 to Policy-map child
PE1(config-pmap-c-qos)#police cir 200 mbps	Police packets @ Committed information rate 200 mbps
PE1(config-pmap-c-qos)#service-policy child	Attaching child policy to Parent
PE1(config-pmap-c-qos)#exit	Exit mode
PE1(config-pmap-qos)#exit	Exit from Policy Map
PE1(config)#router ldp	Enter the Router LDP mode.
PE1(config-router)#targeted-peer ipv4 21.21.21.21	Configure targeted peer
PE1(config-router-targeted-peer)#<null>exit-targeted-peer-mode	Exit Targeted Peer Mode
PE1(config-router)#transport-address ipv4 11.11.11.11	Configure transport address
PE1(config-router)#exit	Exit mode
PE1(config)#interface ce45	Entering Interface Mode
PE1(config-if)#ip address 1.1.1.1/24	Assigning IP Address to interface
PE1(config-if)#label-switching	Enabling Label Switching on the interface.
PE1(config-if)#enable-ldp ipv4	Enabling LDP
PE1(config-if)#exit	Exit mode
PE1(config)#interface lo	Entering loopback Interface Mode
PE1(config-if)#ip address 11.11.11.11/32 secondary	Assigning IP Address to interface
PE1(config-if)#exit	Exit mode
PE1(config)#interface xe2	Entering Interface Mode
PE1(config-if)#switchport	Enabling the Interface as Switchport
PE1(config-if)#mpls-l2-circuit VPWS-VLAN-200 service-template VPWS-Vlan200-Service	Bind the interface to the VC and add the service-template.
PE1(config-if)#mpls-l2-circuit VPWS-VLAN-300 service-template VPWS-Vlan300-Service	Bind the interface to the VC and add the service-template.
PE1(config-if)#service-policy type qos input parent	Assign service-policy to interface on in-direction
PE1(config-if)#exit	Exit mode
PE1(config)#router ospf	Configure the routing process and The Process ID should be a unique positive integer identifying the routing process

PE1(config-router)#network 1.1.1.0/24 area 0.0.0.0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
PE1(config-router)#network 11.11.11.11/32 area 0.0.0.0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
PE1(config-router)#exit	Exit Router Ospf MOde

PE2 Configuration

PE2#configure terminal	Enter configure terminal mode
PE2(config)#hardware-profile filter ingress-ipv6 enable	Enabling Ingress IPv6 group for IPv6 feature
PE2(config)#hardware-profile filter qos-policer enable	Enabling Ingress extended QOS group for hierarchical policer
PE2(config)#qos enable	Enabling QoS
PE2(config)#qos statistics	Enabling Qos statistics
PE2(config)#mpls l2-circuit VPWS-VLAN-200 2000200 11.11.11.11	Create an instance of an MPLS layer 2 virtual circuit
PE2(config)#mpls l2-circuit VPWS-VLAN-300 2000300 11.11.11.11	Create an instance of an MPLS layer 2 virtual circuit
PE2(config)#mpls lsp-model uniform	Configure the MPLS LSP model as Uniform.
PE2(config)#service-template VPWS-Vlan200-Service	Enabling Service Template
PE2(config-svc)#match outer-vlan 200	Match outer vlan 200
PE2(config-svc)#rewrite ingress translate 100 outgoing-tpid dot1.q	Enabling command to configure a match VLAN action for a service template
PE2(config-svc)#exit	Exit mode
PE2(config)#service-template VPWS-Vlan300-Service	Enabling Service Template
PE2(config-svc)#match outer-vlan 300	Match outer vlan 300
PE2(config-svc)#rewrite ingress translate 4000 outgoing-tpid dot1.q	Enabling command to configure a match VLAN action for a service template
PE2(config-svc)#exit	Exit mode
PE2(config)#class-map c0	Enter Class-map mode
PE2(config-cmap-qos)# match cos 0	Matching cos value inside class map
PE2(config-cmap-qos)#exit	Exit mode
PE2(config)#class-map c1	Enter Class-map mode
PE2(config-cmap-qos)#match cos 1	Matching cos value inside class map
PE2(config-cmap-qos)#exit	Exit mode
PE2(config)#class-map c2	Enter Class-map mode
PE2(config-cmap-qos)#match cos 2	Matching cos value inside class map
PE2(config-cmap-qos)#exit	Exit mode
PE2(config)#class-map c3	Enter Class-map mode
PE2(config-cmap-qos)#match cos 3	Matching cos value inside class map
PE2(config-cmap-qos)#exit	Exit mode

PE2(config)#class-map cp1	Enter Class-map mode
PE2(config-cmap-qos)#match vlan 200	Matching vlan inside class map
PE2(config-cmap-qos)#exit	Exit mode
PE2(config)#class-map cp2	Enter Class-map mode
PE2(config-cmap-qos)#match vlan 300	Matching vlan inside class map
PE2(config-cmap-qos)#exit	Exit mode
PE2(config)#policy-map child	Enter policy-map mode
PE2(config-pmap-qos)#class c0	Assign Class c0 to Policy-map child
PE2(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#class c1	Assign Class c1 to Policy-map child
PE2(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#class c2	Assign Class c2 to Policy-map child
PE2(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#class c3	Assign Class c3 to Policy-map child
PE2(config-pmap-c-qos)#police cir 50 mbps eir 150 mbps	Police packets @ Committed information rate 50 mbps
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#policy-map parent	Enter policy-map mode
PE2(config-pmap-qos)#class cp1	Assign Class cp1 to Policy-map parent
PE2(config-pmap-c-qos)#police cir 200 mbps	Police packets @ Committed information rate 200 mbps
PE2(config-pmap-c-qos)#service-policy child	Attaching child policy to Parent
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#class cp2	Assign Class cp2 to Policy-map child
PE2(config-pmap-c-qos)#police cir 200 mbps	Police packets @ Committed information rate 200 mbps
PE2(config-pmap-c-qos)#service-policy child	Attaching child policy to Parent
PE2(config-pmap-c-qos)#exit	Exit mode
PE2(config-pmap-qos)#exit	Exit from Policy Map
PE2(config)#router ldp	Enter the Router LDP mode
PE2(config-router)#targeted-peer ipv4 11.11.11.11	Configure targeted peer
PE2(config-router-targeted-peer)#exit-targeted-peer-mode	Exit Targeted Peer Mode
PE2(config-router)# transport-address ipv4 21.21.21.21	Configure transport address
PE2(config-router)#exit	Exit mode
PE2(config)#interface ce45	Entering Interface Mode
PE2(config-if)#ip address 1.1.1.2/24	Assigning IP Address to interface

PE2(config-if)#label-switching	Enabling Label Switching on the interface.
PE2(config-if)#enable-ldp ipv4	Enabling LDP
PE2(config-if)#exit	Exit mode
PE2(config)#interface lo	Entering loopback Interface Mode
PE2(config-if)#ip address 21.21.21.21/32 secondary	Assigning IP Address to interface
PE2(config-if)#exit	Exit interface mode
PE2(config)#interface xe1	Entering Interface Mode
PE2(config-if)#switchport	Enabling the Interface as Switch port
PE2(config-if)#mpls-l2-circuit VPWS-VLAN-200 service-template VPWS-Vlan200-Service	Bind the interface to the VC and add the service-template.
PE2(config-if)#mpls-l2-circuit VPWS-VLAN-300 service-template VPWS-Vlan300-Service	Bind the interface to the VC and add the service-template.
PE2(config-if)#service-policy type qos input parent	Assign service-policy to interface on in-direction
PE2(config-if)#exit	Exit interface mode
PE2(config)#router ospf	Configure the routing process and The Process ID should be a unique positive integer identifying the routing process
PE2(config-router)#network 1.1.1.0/24 area 0.0.0.0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
PE2(config-router)#network 21.21.21.21/32 area 0.0.0.0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
PE2(config-router)#exit	Exit Router OSPF mode

Validation

PE1

Validate LDP session using following show command:

```
PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
21.21.21.21               ce45       Passive   OPERATIONAL   30    00:05:40
```

Validate virtual circuit status using following command:

```
PE1#show mpls vc-table
VC-ID    VID  Inner-VID  Ac-Intf  Nw-Intf  Out Label  Tunnel-Label  Nexthop      Status
2000200  N/A  N/A        xe2      ce45     24320      3             21.21.21.21  Active
2000300  N/A  N/A        xe2      ce45     24321      3             21.21.21.21  Active
```

Validate QoS configuration and statistics using below commands:

```
PE1#show policy-map interface xe2

Interface xe2
Type QoS statistics status : enabled
```

```
Service-policy (qos) input: parent
---------------------------
Class-map (qos): cp1 (match all)
 match vlan 200
 police cir 200 mbps
 shape 0 kbps (inherited)

     Child Service-policy (qos) : child
     ---------------------------
     Class-map (qos): c0 (match all)
      match cos 0
      police cir 50 mbps eir 150 mbps
           matched      : 168530 packets, 252795000 bytes
           transmitted  : 85295 packets, 127942500 bytes
           dropped      : 83235 packets, 124852500 bytes

     Class-map (qos): c1 (match all)
      match cos 1
      police cir 50 mbps eir 150 mbps
           matched      : 168523 packets, 252784500 bytes
           transmitted  : 85286 packets, 127929000 bytes
           dropped      : 83237 packets, 124855500 bytes

     Class-map (qos): c2 (match all)
      match cos 2
      police cir 50 mbps eir 150 mbps
           matched      : 168558 packets, 252837000 bytes
           transmitted  : 85320 packets, 127980000 bytes
           dropped      : 83238 packets, 124857000 bytes

     Class-map (qos): c3 (match all)
      match cos 3
      police cir 50 mbps eir 150 mbps
           matched      : 168550 packets, 252825000 bytes
           transmitted  : 85310 packets, 127965000 bytes
           dropped      : 83240 packets, 124860000 bytes

     Class-map (qos): class-default (match any)

Class-map (qos): cp2 (match all)
 match vlan 300
 police cir 200 mbps
 shape 0 kbps (inherited)

     Child Service-policy (qos) : child
     ---------------------------
     Class-map (qos): c0 (match all)
      match cos 0
      police cir 50 mbps eir 150 mbps
           matched      : 168597 packets, 252895500 bytes
```

```
           transmitted  : 85336 packets, 128004000 bytes
           dropped      : 83261 packets, 124891500 bytes

     Class-map (qos): c1 (match all)
      match cos 1
      police cir 50 mbps eir 150 mbps
           matched      : 168589 packets, 252883500 bytes
           transmitted  : 85327 packets, 127990500 bytes
           dropped      : 83262 packets, 124893000 bytes

     Class-map (qos): c2 (match all)
      match cos 2
      police cir 50 mbps eir 150 mbps
           matched      : 168625 packets, 252937500 bytes
           transmitted  : 85358 packets, 128037000 bytes
           dropped      : 83267 packets, 124900500 bytes

     Class-map (qos): c3 (match all)
      match cos 3
      police cir 50 mbps eir 150 mbps

     Class-map (qos): class-default (match any)
           matched      : 168589 packets, 252883500 bytes
           transmitted  : 85333 packets, 127999500 bytes
           dropped      : 83256 packets, 124884000 bytes

Service-policy (queuing) output: default-out-policy
Interface Bandwidth 1000000 kbps
----------------------------------
Class-map (queuing): q0
 shape 1000000 kbps (inherited)
 priority level 0
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q1
 shape 1000000 kbps (inherited)
 priority level 1
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q2
 shape 1000000 kbps (inherited)
 priority level 2
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q3
 shape 1000000 kbps (inherited)
 priority level 3
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q4
```

```
 shape 1000000 kbps (inherited)
 priority level 4
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q5
 shape 1000000 kbps (inherited)
 priority level 5
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q6
 shape 1000000 kbps (inherited)
 priority level 6
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q7
 shape 1000000 kbps (inherited)
 priority level 7
 queue-limit 1048576 bytes/8 ms (default)


PE1#show policy-map statistics
Type qos class-map statistics:
+---------------+---------------+----------------+----------------+------------------+
|   Class-map   |   Match pkts  |  Match bytes   |  Dropped pkts  |   Dropped Bytes  |
+---------------+---------------+----------------+----------------+------------------+
xe2
 cp1
   c0            231860          347790000        114528          171792000
   c1            231854          347781000        114531          171796500
   c2            231891          347836500        114533          171799500
   c3            231884          347826000        114534          171801000
 cp2
   c0            231933          347899500        114557          171835500
   c1            231926          347889000        114558          171837000
   c2            231963          347944500        114563          171844500
   class-default 231930          347895000        114555          171832500

Type queuing class-map statistics:
+---------------+---------------+----------------+----------------+------------------+
|   Class-map   |   Total pkts  |  Total bytes   |  Dropped pkts  |   Dropped Bytes  |
+---------------+---------------+----------------+----------------+------------------+
ce45
 q0              5595949         8393932500       229131          343705500
 q1              5596049         8394085500       229228          343851000
 q2              5596147         8394232500       229327          343999500
 q3              2798111         4197172500       114702          172057500
 q4              2798195         4197300000       114762          172147500
 q6              23              1886             0               0
 q7              249             21339            0               0
```

PE2

Validate LDP session using following show command:

```
PE2#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
11.11.11.11               ce45       Active    OPERATIONAL   30    00:06:59
```

Validate virtual circuit status using following command:

```
PE2#show mpls vc-table
VC-ID    VID  Inner-VID  Ac-Intf  Nw-Intf  Out Label  Tunnel-Label  Nexthop      Status
2000200  N/A  N/A        xe1      ce45     24320      3             11.11.11.11  Active
2000300  N/A  N/A        xe1      ce45     24321      3             11.11.11.11  Active
```

Validate QoS configuration and statistics using below commands:

```
PE2#show policy-map interface xe1

Interface xe1
Type QoS statistics status : enabled

Service-policy (queuing) output: default-out-policy
Interface Bandwidth 1000000 kbps
---------------------------------
Class-map (queuing): q0
 shape 1000000 kbps (inherited)
 priority level 0
 queue-limit 1048576 bytes/8 ms (default)
      Output
         Total        : 6205481 packets, 9419929266 bytes
         Green        : 6205548 packets, 9420032490 bytes
         Yellow       : 0 packets, 0 bytes

Class-map (queuing): q1
 shape 1000000 kbps (inherited)
 priority level 1
 queue-limit 1048576 bytes/8 ms (default)
      Output
         Total        : 6205580 packets, 9420081066 bytes
         Green        : 6205651 packets, 9420188844 bytes
         Yellow       : 0 packets, 0 bytes

Class-map (queuing): q2
 shape 1000000 kbps (inherited)
 priority level 2
 queue-limit 1048576 bytes/8 ms (default)
      Output
         Total        : 6205681 packets, 9420260190 bytes
         Green        : 6205798 packets, 9420410472 bytes
         Yellow       : 0 packets, 0 bytes
```

```
Class-map (queuing): q3
 shape 1000000 kbps (inherited)
 priority level 3
 queue-limit 1048576 bytes/8 ms (default)
      Output
         Total        : 3102900 packets, 4710206754 bytes
         Green        : 3102934 packets, 4710258366 bytes
         Yellow       : 0 packets, 0 bytes

Class-map (queuing): q4
 shape 1000000 kbps (inherited)
 priority level 4
 queue-limit 1048576 bytes/8 ms (default)
      Output
         Total        : 3102984 packets, 4710337302 bytes
         Green        : 3103019 packets, 4710388914 bytes
         Yellow       : 0 packets, 0 bytes

Class-map (queuing): q5
 shape 1000000 kbps (inherited)
 priority level 5
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q6
 shape 1000000 kbps (inherited)
 priority level 6
 queue-limit 1048576 bytes/8 ms (default)

Class-map (queuing): q7
 shape 1000000 kbps (inherited)
 priority level 7
 queue-limit 1048576 bytes/8 ms (default)


PE2#show policy-map statistics
Type qos class-map statistics:
+---------------+----------------+----------------+----------------+------------------+
|   Class-map   |   Match pkts   |  Match bytes   |  Dropped pkts  |   Dropped Bytes  |
+---------------+----------------+----------------+----------------+------------------+

Type queuing class-map statistics:
+---------------+----------------+----------------+----------------+------------------+
|   Class-map   |   Total pkts   |  Total bytes   |  Dropped pkts  |   Dropped Bytes  |
+---------------+----------------+----------------+----------------+------------------+
ce45
 q6              29               2378             0                0
 q7              295              25051            0                0
xe1
 q0              6339725          9623710140       0                0
 q1              6339793          9623811846       0                0
```

```
q2              6339857         9623908998      0               0
q3              3169947         4811984100      0               0
q4              3170018         4812088842      0               0
```

CHAPTER 21 Subinterface Queuing

In Qumran devices, every physical port has default eight priority queues and subinterface has default 4 priority queues. Physical port queues are created during initialization while the subinterface queues will be created/deleted when encap is set/unset respectively on subinterface. Whenever QoS feature is enabled, all priority queues of the physical ports/ subinterafce will be configured with certain default egress queuing parameters.

In order to customize the treatment on the priority queues, queuing policy-map infrastructure need to be used.

Configuring Subinterface Queues

Subinterface queues are nothing different then the physical ports queues expect that number of queues assigned to a subinterface can be set via profile and by-default profile1 is set which sets 4 queues to be created for services.

User can configure the service-queue profile via cli "hardware-profile service-queue (profile1 | profile2)".

Profile1 supports 4 new queues creation for services,which is also a default profile. Profile2 supports 8 new queues creation for services.

These queues will be created or deleted when the encap is set or unset on a subinterface respectively. Like and other interface, subinterface has a default ingress egress mapping profile. i.e.dscp-to-queue and dscp-color-to-dscp respectively. Subinterface has default queuing-policy in order to support QoS treatment on the queues.

Mapping profiles (dscp-to-queue and dscp-color-to-dscp) maps packets dscp to/from 8 traffic classes. When the hardware-queues created are 4, 8 traffic classes will be mapped to these 4 hardware-queues implicitly as shown in Table 21-83:

Table 21-83: Traffic class to queue mapping

Traffic class	Queue
0	0
1, 2, 3	1
4, 5	2
6-7	3

This map can be checked via this command:

```
show queue remapping
```

Output:

```
Port queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           2           |
|      3     |           3           |
|      4     |           4           |
|      5     |           5           |
|      6     |           6           |
|      7     |           7           |
```

```
+------------+-----------------------+

Service queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           1           |
|      3     |           1           |
|      4     |           2           |
|      5     |           2           |
|      6     |           3           |
|      7     |           3           |
+------------+-----------------------+
```

When the number of profile 2 is active, number of new queues created will be 8 and the traffic class to hardware queues map will be one to one.

This map can be checked via this command:

```
    show queue remapping
```

Output:

```
Port queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           2           |
|      3     |           3           |
|      4     |           4           |
|      5     |           5           |
|      6     |           6           |
|      7     |           7           |
+------------+-----------------------+

Service queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           2           |
|      3     |           3           |
|      4     |           4           |
|      5     |           5           |
|      6     |           6           |
|      7     |           7           |
+------------+-----------------------+
```

Configuring Default Queuing Policy-Map

When the QoS feature is enabled, all subinterfaces is supplied with a default policy-map of queuing type. The default policy-map is created with the name "default-subif-out-policy" which is reserved and modifying parameters in this policy-map is reflected on all subinterfaces that do not have customized queuing policy-maps. Customized queuing policy-maps can be created and bound to subinterface to treat subinterface differently from the default configuration.

Default queuing-policy can be accessed via following cli:

```
policy-map type queuing default subif-default-out-policy
```

Classes mapped to default queues can be accessed via following cli:

```
class type queuing default (q0|q1|q2|q3)
```

User can configure all the queue parameters like shaping, scheduling, wred, taildrop same as on port. Show commands to verify the config and stats are same. For these configurations please check respective chapters as described in the document.

Displaying Policy-Map Configuration

```
(config)#show pol in xe11.1

Interface xe11.1

Type Queuing policy-map : subif-default-out-policy

Class-map (queuing): q0
 shape 1000000 kbps (inherited)
 priority level 0
 queue-limit 1253376 bytes/10 ms (default)

Class-map (queuing): q1
 shape 1000000 kbps (inherited)
 priority level 1
 queue-limit 1253376 bytes/10 ms (default)
      Output
         Total        : 4109055 packets, 279534060 bytes
         Green        : 4120123 packets, 280222424 bytes
         Yellow       : 0 packets, 0 bytes
      Rate            : 768646.000 kbps

Class-map (queuing): q2
 shape 1000000 kbps (inherited)
 priority level 2
 queue-limit 1253376 bytes/10 ms (default)

Class-map (queuing): q3
 shape 1000000 kbps (inherited)
 priority level 3
 queue-limit 1253376 bytes/10 ms (default)
```

Creating a User-Defined Queuing Policy-Map

Qumran supports the creation of customized policy-map in which all 4 priority queues can be accessed. The following is the command to create a customized default policy-map:

```
(no|) policy-map type queuing NAME
```

Class-maps can be configured matching queues via following cli:

```
(no|) class-map type queuing NAME
```

Match queue/queues in the class-map via following cli :

```
(no|) match queue <0-7>
```

Note: The match queue range 0-7 is valid only for port queues classification.

For service queues/subinterface, the valid range is 0-3.

Once the policy-map and class-maps are configured, class-maps can be configured in the policy-map with the following command:

```
class type queuing NAME
```

Binding a User-Defined Queuing Policy-Map

Customized queuing policy-maps take affect only when the configuration is bound to an interface. Queuing policy-maps can be bound to the port with the following command:

```
service-policy type queuing output NAME
```

Where NAME represents the name of the queuing policy-map.

For example:

```
class-map type queuing data
 match queue 0
!
class-map type queuing signal
 match queue 3
!
class-map type queuing voice
 match queue 1
!
policy-map type queuing configPolicy1
 class type queuing class-default-q
  exit
 class type queuing data
  exit
 class type queuing signal
  exit
 class type queuing voice
  exit
!
interface xe11.1
 service-policy type queuing output configPolicy1
```

Queue(s) which are not matched in any class in a user-defined policy-map, will be mapped to Class-default-q by default. This class-default-q is a by-default created class in a user-defined policy-map.

Displaying Policy-Map Configuration

```
(config-if)#do show policy-map in xe11.1

Interface xe11.1

Type Queuing policy-map : configPolicy1

Class-map (queuing): class-default-q
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 2

Class-map (queuing): data
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 0

Class-map (queuing): signal
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 3

Class-map (queuing): voice
 shape 1000000 kbps (inherited)
 wfq-queue weight 1
 queue-limit 1253376 bytes/10 ms (default)
 match queue 1
      Output
         Total        : 2321147 packets, 157909736 bytes
         Green        : 2337514 packets, 158952312 bytes
         Yellow       : 0 packets, 0 bytes
      Rate            : 773130.375 kbps
```

Displaying Policy-Map Rate Statistics

```
#show policy-map statistics type queuing rate mbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in mbps)  |
+--------------------------------+--------------------+
xe11.1
 voice (q1)                       773.104
```

```
#show policy-map statistics type queuing rate kbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in kbps)  |
+--------------------------------+--------------------+
xe11.1
 voice (q1)                       772400.062
#show policy-map statistics type queuing rate gbps
+--------------------------------+--------------------+
|            Class-map           |    Rate (in gbps)  |
+--------------------------------+--------------------+
xe11.1
 voice (q1)                       0.774
```

Displaying Interface Queue Counters

```
#show interface xe11.1 counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+-----------------+--------+----------+-----------+-----------------+--------------+
| Queue/Class-map | Q-Size |  Tx pkts | Tx bytes  |  Dropped pkts   | Dropped bytes|
+-----------------+--------+----------+-----------+-----------------+--------------+
q0             (E) 1253376  0          0             0                 0
q1             (E) 1253376  1402466359 95367712820   0                 0
q2             (E) 1253376  0          0             0                 0
q3             (E) 1253376  0          0             0                 0
```

Configuration Considerations

- Max 1 level of user defined hierarchy is supported on subinterface.
- Only match queue is allowed in the class in user-define queuing policy-map.
- In user-defined policy-map, all the classes will be in wfq scheduling manner.
- Class-default-q is a self-created class map as part a policy map. It cannot be created nor be destroyed. It will be displayed only when user access it. Executing command "no class-default-q", will un-configure all the configurations of class-default-q.
- User can configure all queuing parameters like weight, priority, queue-limit, wred and shape in a class inside policy.
- Valid match queue and the priority range is 0-3.
- Update is possible in the policy-map except the update of match criteria. Once the class with some match criteria is used in a policy-map, it cannot be updated.
- Subinterface queuing can be achieved via vlan-shaping (match interface) as well as via default queues.
- User-defined policy with match subinterface can only be attached on parent interface if subinterface is not attached to user-defined policy-map.
- If user-defined policy with match subinterface is attached on parent interface, sub-interface's default policy-map and port shaper will be removed implicitly from subinterface.
- If the user-defined-policy is applied on parent interface matching subinterface, traffic will go to the queues created via user-defined-service-policy and the queue stats for subinterface will only be displayed via service-policy. The subinterfaces not matched in the user-defined-service policy will go to their own queues only and not to class-default as happens in case of vlan shaping.

- On encap delete from subinterface, all the qos configuration will be removed implicitly from the subinterafce.
- If the port shaper is applied on parent port and on subinterface as well, minimum shape rate will take effect.
- Queue shape percent for subinterface queues, will be calculated as in following manner:
- Percentage will be calculated from the Effective Max speed, which will be calculated as follows:

    max_speed = parent_ifp->speed.

  If shaper is applied on parent port:

    max_speed = parent_port_shaper

  If shaper is applied on subinterface:

    max_speed = subinterface_shaper

Quality of Service Command Reference

Contents

This document contains this chapter:

CHAPTER 23 Quality of Service Commands

This chapter is a reference for the ingress Quality of Service (QoS) and hierarchical QoS.

- qos statistics
- qos untagged-priority
- queue-limit
- random-detect
- queue shaper
- port shaper
- service-policy type qos
- service-policy type queuing
- set cos
- set dscp
- set precedence
- set queue
- show class-map
- show interface counters
- show policy-map
- show policy-map interface
- show qos-profile
- show qos-profile interface
- show queuing interface
- show running-config qos
- storm-control
- tust dscp
- wfq-queue weight
- vc-qos map-profile
- vpls-qos map-profile

class-map type qos

Use this command to create a class-map of type qos.

Use the no command to remove a class-map.

Note: Class-map without any match qualification behaves similar to default class by matching all the packets on the interface it is attached via service policy.

Note: In a class-map, adding or deleting match criteria will have silent exit and will not proceed with operation.

Note: In match-all class-map, only single value with any criteria can exist. Adding new value for the existing criteria will update the same rule. Multiple values with the same criteria can be added in the “match-any” class-map

Command Syntax

```
class-map (type qos|) (match-any|match-all|) NAME
no class-map (type qos|) (match-any|match-all|) NAME
```

Parameters

NAME	Specify the class map name (Max Size 32)
match-any	Match any parameter (boolean OR)
match-all	Match all parameters (boolean AND)

Default

By default, match type is match-all for any class-map

Command Mode

Configuration Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)# class-map type qos C_QOS1
```

class type qos

Use this command to add a QoS class-map to a qos policy map.

Use the `no command` to remove a QoS class-map from the policy map.

Note: Priority of class in policy-map is as follow:

- Match-all" class-maps will have priorities equal to number of match types specified in class-map “Match-any.”
- Will have lowest priority which will be the same as priority of “match-all” with one match type.
- Only policer action is supported in the class having “match access-grp” criteria in match-any class-map.

Command Syntax

```
class (type qos|) (NAME|class-default)
no class (type qos|) (NAME|class-default)
```

Parameters

NAME	Specify the class map name

Default

By default, class is type qos

Command Mode

Policy-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#
(config)#policy-map type qos PP
(config-pmap-que)#class type qos C_PP_1
```

class type queuing

Use this command to add a queuing class-map to a queuing policy map.

Default queuing class cannot be deleted.

Command Syntax

```
class type queuing default (q0|q1|q2|q3|q4|q5|q6|q7)
```

Parameters

NAME	Specify the class map name
<q0-q7>	Default queue name

Default

No default value is specified

Command Mode

Policy Map type queuing Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#
(config)#policy-map type queuing default default-out-policy
(config-pmap-que)#class type queuing default q0
```

clear qos statistics

Use this command to clear the quality of service (QoS) statistics.

Command Syntax

```
clear qos statistics (interface NAME |)(input | output |) (type (qos | queuing)|)
```

Parameters

NAME	Specify which interface to clear.

Default

By default, type QoS, type queuing class statistics on all interface's will be cleared, if no parameters configured

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#clear qos statistics
#
```

clear interface counters

Use this command to clear all the interface counters.

Command Syntax

```
clear interface counters
```

Parameters

NA

Default

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#clear interface counters
#
```

egress l2 exp encap map

Use this command to map a queue color to the some exp value for L2 traffic.

Use the no form of this command to remove the map.

Note: Color is an optional parameter. If not provided, the same map is set for all colors.

Command Syntax

```
l2 queue <0-7> (color (green|yellow|red)|) exp <0-7>
no l2 queue <0-7> (color (green|yellow|red)|)
```

Parameters

<0-7>	Identifying queue number
color	(green | yellow | red)
<0-7>	EXP value

Default

By default, queue values are one-to-one mapped to Exp. For example, queue 0 exp 0, queue 1 exp 1, and so on.

Command Mode

config-egress-exp-encap-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile exp-encap default (config-egress-exp-encap-map)#l2 queue
2 exp 1
(config-egress-exp-encap-map)#l2 queue 4 color yellow exp 3
```

Color is an optional parameter, so if users do not provide color for all colors, the same EXP is set. If users provide color, then only that specific color egress map is changed. If, however, users provide a map for all colors, as well as maps without color, the map with color will take priority.

For example,

```
(config-egress-exp-encap-map)#no l2 queue 1 color green
(config-egress-exp-encap-map)#no l2 queue 1
```

If a user wants to remove all the mapping of queue (for all colors), then there is no need to provide color, else the user can provide a specific color to remove a specific map.

egress l3 exp encap map

Use this command to map a DSCP value to the some EXP value.

For L3 traffic, use the no form of this command to remove the map.

Command Syntax

```
l3 dscp <0-63> exp <0-7>
no l3 dscp <0-63>
```

Parameters

<0-63>	DSCP value
<0-7>	EXP value

Default

By default, 8 DSCP values are mapped to one exp.

For example: DSCP 0-7 exp 0, DSCP 8-15 exp 1.

Command Mode

config-egress-exp-encap-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile exp-encap default
(config-egress-exp-encap-map)#l3 dscp 20 exp 1
(config-egress-exp-encap-map)#l3 dscp 40 exp 2
```

egress cos map

Use this command to map a queue value to the cos value.

Use the no form of this command to remove the map.

Note: Egress cos map will be taking effect only when remark cos is enabled.

Note: Color is an optional parameter. If not provided, the same map will be set for all colors.

Command Syntax

```
queue <0-7> (color (green|yellow|red)|) cos <0-7>
no queue <0-7> (color (green|yellow|red)|)
```

Parameters

<0-7>	Identifying queue number
color	(green|yellow|red)
<0-7>	CoS value

Default

By default, CoS to queue mapping is one to one.

Command Mode

config-egress-cos-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile queue-color-to-cos default
(config-egress-cos-map)#queue 1 color green cos 5
(config-egress-cos-map)#queue 1 cos 6
```

Color is an optional parameter. So if users do not provide color, for all colors same cos remarking will be set. If user provides color, then only for that specific color egress map will be changed. If user provides map for all colors as well as without color, map with color will take priority.

```
(config-egress-cos-map)#no queue 1 color green
(config-egress-cos-map)#no queue 1
```

If user want to remove all the mapping of queue (for all colors) no need to provide color, else can provide specific color to remove specific map.

egress dscp map

Use this command to map a queue to a dscp value.

Use the no form of this command to remove the map.

Note: Egress dscp map will be taking effect only when remark dscp is enabled.

Note: Color is an optional parameter. If not provided, the same map will be set for all colors.

Command Syntax

```
queue <0-7> (color (green|yellow|red)|) dscp <0-63>
no queue <0-7> (color (green|yellow|red)|)
```

Parameters

<0-7>	Identifying queue number
color	(green|yellow|red)
<0-63>	DSCP value

Default

By default, 8 DSCP values are mapped to one queue.

For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

config-egress-dscp-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile dscp-to-dscp default
(config-egress-dscp-map)#dscp 20 color yellow dscp 40
(config-egress-dscp-map)#dscp 20 dscp 36
```

If user specifies color in map then map will be set for that specific color else for all colors same map will be set.

```
(config-egress-dscp-map)#no dscp 20 color yellow
(config-egress-dscp-map)#no dscp 20
```

If user want to remove all the mapping of dscp (for all colors) no need to provide color, else can provide specific color to remove specific map.

ingress cos map

Use this command to map a cos value to the queue.

Use the no form of this command to remove the map.

Note: Color mapping is fixed: DEI 0 will be mapped to color “green” and DEI 1 will be mapped to color “yellow.”

Command Syntax

```
cos <0-7> queue <0-7>
no cos <0-7>
```

Parameters

<0-7>	CoS value
<0-7>	Identifying queue number

Default

By default, CoS to queue mapping is one to one.

Command Mode

config-ingress-cos-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile cos-to-queue default
(config-ingress-cos-map)#cos 1 queue 2
```

ingress dscp map

Use this command to map a dscp value to the queue.

Use the no form of this command to remove the map.

Note: You can “remark” the dscp value for the incoming traffic at ingress via map by setting the last “dscp” field. You still need to match traffic with the incoming dscp value in the class-map even if you are remarking them at ingress via a dscp map. Traffic will be received with remarked dscp value at egress if no egress dscp map is applied. If an egress dscp map (such as dscp-to-dscp) is applied at the egress port, and dscp remarking is enabled, dscp will be remarked again according to the mapping given for the remarked dscp (the dscp value given in ingress dscp map).

Note: Last “dscp” parameter is remark_dscp value, which if provided will be set as the same ingress dscp value. Color is an optional parameter. If not provided, it will be set as the default value. Please refer the Configuration Guide for the default value table.

Command Syntax

```
dscp <0-63> queue <0-7> (color (green|yellow|red)|) (dscp <0-63>|)
no dscp <0-63>
```

Parameters

<0-63>	DSCP value
<0-7>	Identifying queue number
color	(green|yellow|red)

Default

By default, 8 DSCP values are mapped to one queue.

For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

config-ingress-dscp-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile dscp-to-queue default
(config-ingress-dscp-map)#dscp 1 queue 2
```

ingress exp map

Use this command to map a exp value to the queue.

Use the no form of this command to remove the map.

Note: Color is an optional parameter. If not provided, color will be set to green.

Command Syntax

```
exp <0-7> queue <0-7> (color (green|yellow|red)|)
no exp <0-7>
```

Parameters

<0-7>	EXP value
<0-7>	Identifying queue number
color	(green|yellow|red)

Default

By default, EXP to queue mapping is one to one.

Command Mode

config-ingress-exp-queue-map

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile exp-to-queue default
(config-ingress-exp-queue-map)#exp 1 queue 4 color green
(config-ingress-exp-queue-map)#exp 2 queue 3
```

match access-group

Use this command to classify the group based on the access group.

Use the `no command` remove access group match criteria from a class map

Note: Match access-group is allowed only in “match-any” class type.

When match access-grp is configured, no more match criteria can be supported in the class-map.

When access-list is being used in class-map for match, only “permit rules” are allowed in the access-list.

Command Syntax

`match access-group` NAME

Parameters

NAME	Specify the access group name

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# class-map match-any class_acl
(config-cmap-qos)# match access-group my_acl
```

match cos

Use this command to classify the traffic based on cos

Use the `no command` to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on cos using the command `match cos 2,4,6` and remove the match configuration using the command `no match cos 2-6.`

Command Syntax

```
match cos WORD
no match cos (WORD|all)
```

Parameters

`WORD`	CoS value or list of specified CoS values. Valid values are from 0 to 7.
`all`	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos 1
```

match cos inner

Use this command to classify the traffic based on inner cos.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on inner cos using the command `match cos inner 2,4,6` and remove the match configuration using the command `no match cos inner 2-6`.

Command Syntax

```
match cos inner WORD
no match cos inner (WORD|all)
```

Parameters

`WORD`	Inner CoS value or list of specified CoS values. Valid values are from 0 to 7.
`all`	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos inner 1
```

match dscp

Use this command to classify the traffic based on dscp.

Use the `no` command to remove the configured dscp value.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on dscp using the command `match dscp 2,4,6` and remove the match configuration using the command `no match dscp 2-6`.

Match dscp cannot be configured in the class-map where match precedence is already configured.

Command Syntax

```
match dscp [WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31| af32 | af33 |
  af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6| cs7 | default | ef]
```

```
no match dscp ([WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33
  | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4  cs5 | cs6 | cs7 | default | ef]|all)
```

Parameters

`WORD`	<0-63> List of DSCP values.
`af11`	AF11 dscp (001010).
`af12`	AF12 dscp (001100)
`af13`	AF13 dscp (001110)
`af21`	AF21 dscp (010010)
`af22`	AF22 dscp (010100)
`af23`	AF23 dscp (010110)
`af31`	AF31 dscp (011010)
`af32`	AF32 dscp (011100)
`af33`	AF33 dscp (011110)
`af41`	AF41 dscp (100010)
`af42`	AF42 dscp (100100)
`af43`	AF43 dscp (100110)
`cs1`	CS1(precedence 1) dscp (001000)
`cs2`	CS2(precedence 2) dscp (010000)
`cs3`	CS3(precedence 3) dscp (011000)
`cs4`	CS4(precedence 4) dscp (100000)
`cs5`	CS5(precedence 5) dscp (101000)
`cs6`	CS6(precedence 6) dscp (110000)
`cs7`	CS7(precedence 7) dscp (111000)
`default`	Default dscp (000000)
`ef`	EF dscp (101110)
`all`	Delete all matched DSCP values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS7
(config-cmap-qos)#match dscp 48
```

match ethertype

Use this command to classify the traffic based on the ethertype.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier.

Qualifying the TPID values like 0x8100, 0x88A8, 0x9100 and 0x9200 etc as ethertype will not match if the traffic is flowing with the same TPId in the network.

Command Syntax

```
match ethertype WORD
no match ethertype(WORD|all)
```

Parameters

WORD	Enter ethertype <0x600 to 0xffff)> or list of ethertype separated by commas. For example, 0x806,0x8035 etc.
all	Delete all ethertype entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match ethertype 0x806
```

match ip rtp

Use this command to configure a class map to use the Real-Time Protocol (RTP) port as a match criteria.

Use the `no command` to remove the RTP port as a match criteria.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on RTP port using the command `match ip rtp 5000,7000,9000` and remove the match configuration using the command `no match ip rtp 5000-9000`.

Command Syntax

```
match ip rtp WORD
no match ip rtp (WORD|all)
```

Parameters

`WORD`	Specify User Datagram Protocol (UDP) or list of UDP ports that are using RTP. Valid values are from 2000 to 65535.
`all`	Delete all matched IP RTP values.

Default

No default value is specified

Command Mode

Class-map type qos

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match ip rtp 2300
```

match ipv6 dscp

Use this command to classify the ipv6 traffic based on DSCP.

Use the no command to remove the configured dscp value.

Note the following:

- The match commands which accept range have silent exit which makes removal of these match configuration easier. For example, classify the traffic based on dscp using the command `match dscp 2,4,6` and remove the match configuration using the command `no match dscp 2-6`.
- The `match ipv6 dscp` command cannot be configured in the class-map where match ipv6 precedence is already configured.
- Any `match ipv6` commands cannot be configured in the class-map where `match ipv4` commands are already configured.

Command Syntax

```
match ipv6 dscp [WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31| af32 | af33
  | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6| cs7 | default | ef]
no match ipv6 dscp ([WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
  af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4cs5 | cs6 | cs7 | default |
  ef]|all)
```

Parameters

`WORD`	<0-63> List of DSCP values.
`af11`	AF11 dscp (001010).
`af12`	AF12 dscp (001100)
`af13`	AF13 dscp (001110)
`af21`	AF21 dscp (010010)
`af22`	AF22 dscp (010100)
`af23`	AF23 dscp (010110)
`af31`	AF31 dscp (011010)
`af32`	AF32 dscp (011100)
`af33`	AF33 dscp (011110)
`af41`	AF41 dscp (100010)
`af42`	AF42 dscp (100100)
`af43`	AF43 dscp (100110)
`cs1`	CS1 (precedence 1) dscp (001000)
`cs2`	CS2 (precedence 2) dscp (010000)
`cs3`	CS3 precedence 3) dscp (011000)
`cs4`	CS4 (precedence 4) dscp (100000)
`cs5`	CS5 (precedence 5) dscp (101000)
`cs6`	CS6 (precedence 6) dscp (110000)
`cs7`	CS7 (precedence 7) dscp (111000)

`default`	Default dscp (000000)
`ef`	EF dscp (101110)
`all`	Delete all matched DSCP values

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config)#class-map type qos C_QOS7
(config-cmap-qos)#match ipv6 dscp 48
```

match ipv6 layer4

Use this command to classify the IPv6 traffic based on layer4 protocol src/dest port value.

Use the no command to remove the match configuration.

Please note the following:

- The match commands which accept range have silent exit which makes removal of these match configuration easier. Only one type of layer 4 matching criteria is supported per class-map.
- Any `match ipv6` commands cannot be configured in the class-map where `match ipv4` commands are already configured.

Command Syntax

```
match ipv6 layer4 (tcp|udp|any) (source-port|destination-port) WORD
no match ipv6 layer4 (((tcp|udp|any) (source-port|destination-port) WORD) |all)
```

Parameters

`tcp`	Specify TCP protocol
`udp`	Specify UDP protocol
`any`	Specify ANY protocol - TCP/UDP
`source-port`	Specify source TCP/UDP port
`destination-port`	Specify destination TCP/UDP port
`WORD`	Enter TCP/UDP port value <1-65535> or range of values separated by commas such as 1 or 1,4-5 or 50,51,52
`all`	Delete all layer4 port entries

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match ipv6 layer4 tcp source-port 1
```

match ipv6 precedence

Use this command to IPv6 traffic classification based on precedence.

Use the no command to remove the match configuration.

Please note the following:

- The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on precedence using the command match ipv6 precedence 2,4,6 and remove the match configuration using the command no match ipv6 precedence 2-6.
- The `match ipv6 precedence` command cannot be configured in the class-map where match ipv6 dscp is already configured.
- Any `match ipv6` commands cannot be configured in the class-map where `match ipv4` commands are already configured.

Command Syntax

```
match ipv6 precedence [WORD | critical | flash | flash-override | immediate |
  internet | network | priority | routine]
no match ipv6 precedence ([WORD | critical | flash | flash-override| immediate |
  internet | network | priority | routine]|all)
```

Parameters

`word`	IP precedence value
`critical`	Critical precedence
`flash`	Flash precedence
`flash-override`	Flash override precedence immediateImmediate precedence internetInternetwork control precedence networkNetwork control precedence
`priority`	Priority precedence
`routine`	Routine precedence
`all`	Delete all matched IP precedence values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config)# class-map my_test
(config-cmap-qos)#match ipv6 precedence critical
```

match layer4

Use this command to classify the traffic based on layer4 protocol src/dest port value.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. Only one type of layer4 matching criteria is supported per class-map.

Command Syntax

```
match layer4 (tcp|udp|any) (source-port|destination-port) WORD
no match layer4 (((tcp|udp|any) (source-port|destination-port) WORD) |all)
```

Parameters

`tcp`	Specify TCP protocol
`udp`	Specify UDP protocol
`any`	Specify ANY protocol – TCP/UDP
`source-port`	Specify source TCP/UDP port
`destination-port`	Specify destination TCP/UDP port
`WORD`	Enter TCP/UDP port value <1-65535> or range of values separated by commas. e.g. 1 or 1,4-5 or 50,51,52
`all`	Delete all layer4 port entries

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match layer4 tcp source-port 1
```

match mpls

Use this command to classify the traffic based on the top mpls exp value.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier.

Command Syntax

```
match mpls experimental topmost WORD
no match mpls experimental topmost (WORD|all)
```

Parameters

WORD	Enter EXP value <0-7> or range of exp values seperated by commas. e.g. 2 or 2,4-5 or 3,4,5 or 2-4,5-7 etc.
all	Delete all exp values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)# match mpls experimental topmost 3
```

match precedence

Use this command to traffic classification based on precedence.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on precedence using the command `match precedence 2,4,6` and remove the match configuration using the command `no match precedence 2-6`.

Match precedence cannot be configured in the “match-all” class-map where match dscp is already configured.

Command Syntax

```
match precedence [WORD | critical | flash | flash-override | immediate | internet |
  network | priority | routine]
no match precedence ([WORD | critical | flash | flash-override| immediate |
  internet | network | priority | routine]|all)
```

Parameters

`word`	IP precedence value
`critical`	Critical precedence
`flash`	Flash precedence
`flash-override`	Flash override precedence
`immediate`	Immediate precedence
`internet`	Internetwork control precedence
`network`	Network control precedence
`priority`	Priority precedence
`routine`	Routine precedence
`all`	Delete all matched IP precedence values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# class-map my_test
(config-cmap-qos)#match precedence critical
```

match vlan

Use this command to classify the traffic based on a VLAN.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on VLAN using the command `match vlan 2,4,6` and remove the match configuration using the command `no match vlan 2-6`.

Command Syntax

```
match vlan WORD
no match vlan (WORD|all)
```

Parameters

`WORD`	Enter VLAN ID <1-4094> or range of VLAN ID's separated by commas. For example, 2 or 2,4-5 or 50,51,52 or 100-120,122-130 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan 100
```

match vlan inner

Use this command to classify the traffic based on the inner VLAN.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on the inner VLAN using the command `match vlan inner 2,4,6` and remove the match configuration using the command `no match vlan inner 2-6`.

Command Syntax

```
match vlan inner WORD
no match vlan inner (WORD|all)
```

Parameters

`WORD`	Enter VLAN ID <1-4094> or list of VLAN ID's separated by commas. For example, 2,4 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan inner 1
```

police

Use this command to configure policing of the data rates for a particular class of traffic.

Use the no command to remove a policing configuration.

Note: Committed Information Rate (CIR) and Excess Information Rate (EIR) can only be whole numbers.

The default burst is 5 ms traffic of the configured rate. Burst configured in milliseconds and microseconds are converted in kbytes by calculating it with input rates.

Police rate (cir/eir) value in percentage is only applicable on physical interfaces.

Command Syntax

For Qumran MX:

```
police (colour-blind | colour-aware|) (cir) (<1-720000000> (kbps|mbps|gbps) |
  percent <1-100>)((eir (<1-720000000> (kbps|mbps|gbps) | percent <1-100>)|)((bc)
  <1-4161> (kbytes|mbytes|ms|us)|)((be) <1-4161> (kbytes|mbytes|ms|us)|))
no police (colour-blind | colour-aware|) (cir) (<1-720000000> (kbps|mbps|gbps) |
  percent <1-100>)((eir (<1-720000000> (kbps|mbps|gbps) | percent <1-100>)|)((bc)
  <1-4161> (kbytes|mbytes|ms|us)|)((be) <1-4161> (kbytes|mbytes|ms|us)|))
```

For Qumran AX:

```
police (colour-blind | colour-aware|) (cir) (<1-500000000> (kbps|mbps|gbps) |
  percent <1-100>)((eir (<1-500000000> (kbps|mbps|gbps) | percent <1-100>)|)((bc)
  <1-4161> (kbytes|mbytes|ms|us)|)((be) <1-4161> (kbytes|mbytes|ms|us)|))
no police (colour-blind | colour-aware|) (cir) (<1-500000000> (kbps|mbps|gbps) |
  percent <1-100>)((eir (<1-500000000> (kbps|mbps|gbps) | percent <1-100>)|)((bc)
  <1-4161> (kbytes|mbytes|ms|us)|)((be) <1-4161> (kbytes|mbytes|ms|us)|))
```

Parameters

colour-blind	Do not police on color.
colour-aware	Do police on color.
cir	Committed information rate.
eir	Excess information rate.
kbps	Specify the units of kbps per second.
mbps	Specify the units of mbps per second.
gbps	Specify the units of gbps per second.
bc <1-4161>	Burst rate committed.
be <1-4161>	Burst rate extended.
ms	Specify the units of bc/be in milliseconds.
us	Specify the units of bc/be in microseconds.

Default

By default, policer type is colour-blind

Command Mode

Policy-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map type qos 2345
(config-pmap-qos)#class type qos 2345
(config-pmap-c-qos)# police cir 2 mbps eir 4 mbps bc 2 mbytes be 4 mbytes
```

policy-map

Use this command to create a policy map and enter policy-map mode.

Use the no form of the command to remove a policy map.

Note: You cannot delete a policy map if it is attached to an interface.

Command Syntax

```
policy-map {NAME | (type (qos |queuing default) NAME)}
no policy-map {NAME | (type (qos |queuing default) NAME)}
```

Parameters

NAME	Policy map name (maximum 32 characters)
qos	QoS policy map
queuing	Queuing policy map

Default

No default value is specified

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#
(config)#policy-map type qos PQOS
```

priority level <0-7>

Use this command to configure a single output queuing class as the priority queue.

Use no command to unset the priority level from the queue.

Strict priority mode supports 8 level, i.e., 0 to 7. The queue is constructed such that a higher priority level has a higher priority.

If more than one queue is in the same level, then there will be fair queuing between those queues.

On qos-enable, all the queues will be in strict-priority. After changing the mode or un-setting the priority, queues will be set for WFQ mode with the default weight 1. To set them again in strict priority, the user needs to configure them manually.

Command Syntax

```
priority level <0-7>
no priority level
```

Parameters

<0-7>	Priority level

Default

No default value is specified

Command Mode

Policy map-class type queuing mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#policy-map type queuing default default-out-policy
(config-pmap-que)#class type queuing default q0
(config-pmap-c-que)#priority level 2
```

priority (QoS)

Use this command to set the user priority for the class attached to this policy-map

Use the no parameter with this command to unset the priority value

Note: The higher the priority number, higher the priority for the class in a policy-map.

User configured priority takes effect over default priority.

Command Syntax

```
priority <1-1000>
no priority
```

Parameters

<1-1000>	Priority value

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#priority 20
```

qos (enable | disable)

Use this command to globally enable or disable Quality-of-Service (QoS).

Note: Enabling or disabling QoS is a disruptive operation, stopping all traffic on ports which causes traffic loss.

Command Syntax

```
qos (enable | disable)
```

Parameters

None

Default

By default, QoS is disabled

Command Mode

Configure

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)# qos enable

(config)#qos disable
```

qos map-profile

Use this command to attach (map) a profile to an interface.

Use the no form of this command to remove a profile.

Note: By-default, “default” profiles are attached on their supported interfaces (cos-to-queue and queue-to-cos on L2 interfaces and dscp-to-queue and dscp-to-dscp on L3 interfaces).

You can create and attach your own profile to supported interfaces. After removing a user-defined profiles from an interface, the “default” profile is applied.

Command Syntax

```
qos map-profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | dscp-to-dscp |
  exp-encap) NAME
no qos map-profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | dscp-to-
  dscp | exp-encap) NAME
```

Parameters

cos-to-queue	Profile for cos to queue map
dscp-to-queue	Profile for dscp to queue map
queue-color-to-cos	Profile for queue color to cos map
dscp-to-dscp	Profile for inDscp to outDscp map
exp-encap	Profile for EXP encapsulation map
exp-to-queue	Profile for EXP to queue map
NAME	Profile map name (maximum 32 characters)

Default

By default, the default cos-to-queue-profile is applied to an L2 interface, and the default dscp-to-queue profile is attached to an L3 interface.

Command Mode

Interface modes

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config-if)#qos map-profile cos-to-queue cos-map
(config-if)#qos map-profile dscp-to-queue dscp-map
(config-if)#qos map-profile queue-color-to-cos egress-cos-map
(config-if)#qos map-profile dscp-to-dscp dscp-dscp-map
(config-if)#qos map-profile exp-encap exp-encap-map
```

qos profile

Use this command to create new profiles or to update “default” profiles.

Use the no form of this command to remove the profiles.

Note: “default” profiles can only be updated and not be deleted. User can create/delete user-defined profiles.

Only “default” exp-to-queue profile is supported.

Note: “exp-encap” profile will be ineffective on tunnels with only 2 nodes with PHP configuration.

Command Syntax

```
qos profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | dscp-to-dscp |
  exp-encap)(NAME|default)
no qos profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | dscp-to-dscp |
  exp-encap)NAME
qos profile exp-to-queue default
```

Parameters

`cos-to-queue`	Profile for cos to queue map
`dscp-to-queue`	Profile for dscp to queue map
`queue-color-to-cos`	Profile for queue color to cos map
`dscp-to-dscp`	Profile for inDscp to outDscp map
`exp-encap`	Profile for the exp encapsulation map
`exp-to-queue`	Profile for exp to queue map
`NAME`	Profile map name (maximum 32 characters)

Default

By default, “default” profile is created for all the profile types. These profiles can only be updated by the user neither be created nor be destroyed.

Command Mode

Configure modes

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

To create a new profile:

```
(config)#qos profile cos-to-queue cos-map
(config)#qos profile dscp-to-queue dscp-map
(config)#qos profile queue-color-to-cos egress-cos-map
(config)#qos profile dscp-to-dscp dscp-dscp-map
(config)#qos profile exp-encap exp-encap-map
```

To update the “default” profile:

```
(config)#qos profile cos-to-queue default
(config)#qos profile dscp-to-queue default
(config)#qos profile queue-color-to-cos default
(config)#qos profile dscp-to-dscp default
(config)#qos profile exp-encap default
(config)#qos profile exp-to-queue default
```

qos red-drop-disable

Use this command to disable red packet drop in the system. Red packets are dropped in the system by default to achieve ingress rate limiting via policer and storm control. However, this command is used when there is no use-case for rate limiting traffic and red packets need to be allowed in the system

Use the no form of this command to enable red packet drop.

Command Syntax

```
qos red-drop-disbale
no qos red-drop-disable
```

Parameters

None

Defaults

By default, red packet drop is enabled.

Command Mode

Configure

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)# qos red-drop-disable
(config)#no qos red-drop-disable
```

qos remark

Use this command to enable remarking of the Class of service (CoS) and Differentiated Services Control Protocol (DSCP) set by the egress map.

Use the no command to disable remarking of the CoS and DSCP.

Command Syntax

In Config mode :

```
qos remark (cos|dscp)
no qos remark (cos|dscp)
```

In interface mode:

```
qos remark (cos|dscp)(enable|disable)
no qos remark (cos|dscp)
```

Parameters

`type`	Remarking type, e.g. CoS or DSCP
`(enable|disable)`	Remarking action

Default

By default, remarking is disabled.

Command Mode

Configure Mode

Interface Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#qos remark cos
(config)#qos remark dscp
(config-if)# qos remark cos disable
(config-if)# qos remark cos enable
(config-if)# qos remark dscp disable
```

Interface remarking will take priority over global remarking configurations.

qos statistics

Use this command to enable Quality of Service (QoS) statistics.

Use the no command to disable QoS statistics

Note: Class-map statistics is cleared whenever the match or action property of the class is modified dynamically.

Command Syntax

```
qos statistics
no qos statistics
```

Parameters

None

Default

By default, QoS statistics is disabled

Command Mode

Configure Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#qos statistics
(config)#
```

qos untagged-priority

Use this command to set internal priority for untagged traffic on L2 ports.

Use the no form of the command to remove the configuration.

Note: This command is applicable only on L2 ports.

Command Syntax

```
qos untagged-priority <0-7>
no qos untagged-priority
```

Parameters

qos	Quality of Service
untagged-priority	Internal priority for untagged traffic
<0-7>	Value

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#interface xe1
(config-if)#qos untagged-priority 3
```

queue-limit

Use this command to configure tail drop by setting queue limits on egress queues.

Use the `no command` to remove a queue limit.

Command Syntax

```
queue-limit (<1-629145600>) (packets|bytes|kbytes|mbytes|ms)
no queue-limit
```

Parameters

`<1-629145600>`	Specify queue-limit in packets, bytes, or Kilobytes.
	Max value for bytes is min 1024, max 629145600
	Max value for kilobytes is 614400
	Max value for megabytes is 600, Max value for packets is 614400
`packets`	Specify the units of queue-limit in packets
`bytes`	Specify the units of queue-limit in bytes
`kbytes`	Specify the units of queue-limit in kilobytes
`mbytes`	Specify the units of queue-limit in mega-bytes
`ms`	Specify the units of queue-limit in milliseconds

Default

Default queue size is 62914560 bytes

Command Mode

Policy-class-map-queue mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map type queuing default P1
(config-pmap-que)#class type queuing default q1
(config-pmap-c-que)# queue-limit 1 mbytes
```

random-detect

Use this command to configure weighted random early detection (WRED).

Use the no command to remove a WRED configuration.

Command Syntax

```
random-detect (green (minimum-threshold|)< 1-629145600>
  (bytes|kbytes|mbytes|ms|packets)(maximum-threshold|) <1-629145600>
  (bytes|kbytes|mbytes|ms|packets) (drop-probability <1-100>|) yellow (minimum-
  threshold|) < 1-629145600> (bytes|kbytes|mbytes|ms|packets)(maximum-threshold|) <
  1-629145600> (bytes|kbytes|mbytes|ms|packets)(drop-probability <1-100>|)(weight
  <1-31>|))
no random-detect
```

Parameters

minimum-threshold	
	Specify the minimum threshold. In the range of <1-629145600>
maximum-threshold	
	Specify the maximum threshold. In the range of <1-629145600>
packets	Specify the units of queue-limit in packets – range (min 1, max 614400)
bytes	Specify the units of threshold in bytes – range (min 1024, max 629145600)
kbytes	Specify the units of threshold in kilobytes – range (min 1, max 614400)
mbytes	Specify the units of threshold in mega-bytes – range (min 1, max 600)
ms	Specify the units of threshold in milliseconds – range (min 1, max 50)
	Threshold value in ms will be calculated from interface-speed and will be converted into bytes
drop-probability	
	Drop-probability is the fraction of packets dropped when the average queue depth is at the maximum threshold.It can be configured per color Specify the drop-probability in the range <1-100>
weight	Configures the weight factor used in calculating the average queue length. Specify the weight in the range <1-31>. Value specified will be set for all colors

Default

No default value is specified

Command Mode

Policy-class map queue mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map type queuing default P1
```

```
(config-pmap-que)#class type queuing q1
(config-pmap-c-que)# random-detect minimum-threshold 1000 mbytes maximum-
threshold 2000 mbytes
```

queue shaper

Use this command to configure shaping on an egress queue to impose a maximum rate on it.

Use the `no command` to remove a shaping configuration.

Note: Minimum configurable queueing shape rate is 469 Kbps and maximum queuing shape rate is 483 Gbps. Granularity is 469 Kbps for low range and 1.56 % for higher range.

Command Syntax

```
queue shaper (<1-483000000>(kbps|mbps|gbps) | percent <1-100>)
no queue shaper (<1-483000000> (kbps|mbps|gbps) | percent <1-100>)
```

Parameters

`<1-483000000>`	Shaping is based on an average rate. Average rate for shaping in the range of `<1-483000000>.Min shape rate configured is 469 kbps and max shape rate configured is 483 gbps.`
`kbps`	Specify the units of kbps per second
`mbps`	Specify the units of mbps per second
`gbps`	Specify the units of gbps per second
`percent`	Specify the percentage from 1 to 100

Default

No default value is specified

Command Mode

Policy-class-map queue mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map type queuing default default-out-policy
(config-pmap-que)# class type queuing default q0
(config-pmap-c-que)# queue shaper percent 25
(config-pmap-c-que)#
```

port shaper

Use this command to configure shaping on an egress port to impose a maximum rate on it.

Use the no form of the command to remove a shaping configuration.

Note: Minimum configurable port shape rate is 52 Kbps with Granularity of 52 Kbps and maximum shape rate is 1000 Gbps, but applicable maximum rate may be speed of interface.

Command Syntax

```
port shaper rate <1-1000000000> (kbps|mbps|gbps)
no port shaper rate
```

Parameters

`<1-1000000000>`	Specify rate for shaping in the range of `<1-1000000000>. Min shape rate configured on port is 52kbps and max shape rate configured on port is 1000gbps`
`kbps`	Specify the units of kbps per second.
`mbps`	Specify the units of mbps per second.
`gbps`	Specify the units of gbps per second.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# interface xe11
(config-if)# port shaper rate 100 mbps
```

service-policy type qos

Use this command to attach a service-policy of type qos to the interface.

Use the `no` command to remove a service-policy from an interface.

Command Syntax

```
service-policy type qos input NAME
no service-policy type qos input NAME
```

Parameters

`type`	Specify whether the policy map is of type qos.
`NAME`	Specify the policy map to attach to this interface.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#int xe3
(config-if)#service-policy type qos input PQOS
```

service-policy type queuing

Use this command to attach a service-policy of type queuing to the interface.

Use the no command to remove a service-policy from an interface.

Command Syntax

```
service-policy type queuing output NAME
no service-policy type queuing output NAME
```

Parameters

type	Specify whether the policy map is of type queuing.
NAME	Specify the policy map to attach to this interface.

Default

By default, default-out-policy is attached on all interface

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#int xe3
(config-if)#service-policy type queuing output PQOS
```

set cos

Use this command for matching traffic classes set action as change cos in the egress packet to the prescribed value.

Use the `no command` to remove the assigned value from the class.

Note: This command only applies to normal switch ports of type trunk/hybrid. This command does not apply to AC, CEP, or PNP ports. See the qos map-profile command for options for these types of ports.

Command Syntax

```
set cos <0-7>
no set cos <0-7>
```

Parameters

`<0-7>`	CoS value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map-class-qos mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#policy-map my_policy1
(config-pmap-qos)#class traffic_class2
(config-pmap-c-qos)#no set cos 3
(config-pmap-c-qos)#
```

set dscp

Use this command for matching traffic classes set action as change DSCP in the egress packet to the prescribed value.

Use the no command to remove the assigned value from the class

Command Syntax

```
set dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef )
no set dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41|
  af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef )
```

Parameters

<0-63>	DSCP value
af11	DSCP (001011) decimal value 11
af12	DSCP (001100) decimal value 12
af13	DSCP (001101) decimal value 13
af21	DSCP (010101) decimal value 21
af22	DSCP (010110) decimal value 22
af23	DSCP (010111) decimal value 23
af31	DSCP (011111) decimal value 31
af32	DSCP (010000) decimal value 32
af33	DSCP (010001) decimal value 33
af41	DSCP (101001) decimal value 41
af42	DSCP (101010) decimal value 42
af43	DSCP (101011) decimal value 38
cs1	(Precedence 1) DSCP (001000) decimal value 8
cs2	(Precedence 2) DSCP (010000) decimal value 16
cs3	(Precedence 3) DSCP (011000) ecimal value 24
cs4	(Precedence 4) DSCP (100000) decimal value 32
cs5	(Precedence 5) DSCP (101000) decimal value 40
cs6	(Precedence 6) DSCP (110000) decimal value 48
cs7	(Precedence 7) DSCP (111000) decimal value 56
default	DSCP (000000) decimal value 0
ef	DSCP (101110) decimal value 46

Default

No default value is specified

Command Mode

Policy-map-class qos mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set dscp af12
```

set precedence

Use this command for matching traffic classes set action as change precedence in the egress packet to the prescribed value.

Use the `no command` to leave the precedence value unchanged for the class

Command Syntax

```
set (precedence (<0-7>| critical| flash | flash-override|immediate|internet|
  network| priority| routine))
no set (precedence (<0-7>| critical| flash | flash-override|immediate|internet|
  network| priority| routine))
```

Parameters

`<0-7>`	Specify IP precedence value to assign for this class of traffic
`critical`	Critical precedence
`flash`	Flash precedence
`flash-override`	Flash override precedence
`immediate`	Immediate precedence
`internet`	Internetwork control precedence
`network`	Network control precedence
`priority`	Priority precedence
`routine`	Routine precedence

Default

No default value is specified

Command Mode

Policy-map-class qos mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map policy1
(config-pmap-qos)# class class2
(config-pmap-c-qos)# set precedence 3
(config-pmap-c-qos)#
```

set queue

Use this command for matching traffic classes set action as change cos in the egress packet to the prescribed value.

Use the `no command` to remove the assigned value from the class.

Command Syntax

```
set queue <0-7>
no set queue <0-7>
```

Parameters

`<0-7>`	Specify queue value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map-class qos mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# set queue 3
(config-pmap-c-qos)#
```

show class-map

Use this command to display qos/queuing class maps.

Command Syntax

```
show class-map (type (qos|queuing)|) (NAME|)
```

Parameters

NAME	Specify the named class map

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#show class-map c1
  Type qos class-maps
  ===================
      class-map c1
         match cos 3
```

show interface counters

Use this command to see the interface counters.

Command Syntax

```
show interface IFNAME counters queue-stats
```

Parameters

IFNAME	Interface name.

Command Mode

Exec

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#show interface xe1 counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+---+------+--------+---------+---------+-----------+
| Q | Q-Sz | Tx pkt | Tx byte | Drp pkt | Drop byte |
+---+------+--------+---------+---------+-----------+
q0   629160 100      12000     0         0
q1   629160 0        0         0         0
q2   629160 0        0         0         0
q3   629160 0        0         0         0
q4   629160 0        0         0         0
q5   629160 0        0         0         0
q6   629160 0        0         0         0
q7   629160 0        0         0         0
```

show policy-map

Use this command to display:

1. Type qos/queuing policy-map
2. Non zero statistics for type qos or queuing classes on interfaces

Command Syntax

```
show policy-map (NAME | statistics (type (qos|queuing(default|))|))
show policy-map (type (qos|queuing)|)
show policy-map interface NAME (statistics (type (qos|queuing)|))
```

Parameters

`qos`	Type qos policy-map
`statistics`	Displays QoS statistics.
`queuing`	Type queuing policy-maps
`default`	Default queue of the port
`Interface`	Interface on which to get policy-map statistics

Command Mode

Exec and Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

Examples

```
#show policy-map A

Type qos policy-maps
====================

policy-map A
 class A
  set cos 3
  exit
 class B
  exit

#show policy-map asd

Type queuing policy-maps
========================

policy-map type queuing default asd
 class type queuing default q0
  priority level 0
```

```
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
 class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit

#show policy-map statistics type qos
+-----------+------------+-------------+--------------+---------------+
| Class-map | Match pkts | Match bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
xe1
 A           11744033     17616049500       -                -

#show policy-map statistics type queuing
+-----------+------------+-------------+--------------+---------------+
| Class-map | Total pkts | Total bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
xe2
 q3          503336       755148000         0                0

#show policy-map statistics type queuing default
+-----------+------------+-------------+--------------+---------------+
| Class-map | Total pkts | Total bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
xe2
 q3          837204       1255813500        0                0
#

#show policy-map

Type qos policy-maps
====================

policy-map A
 class A
  set cos 3
  exit
 class B
  exit
Type queuing policy-maps
```

```
=======================

policy-map type queuing default asd
 class type queuing default q0
  priority level 0
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
 class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 0
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
 class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit
#show policy-map type qos

Type qos policy-maps
====================
```

```
policy-map A
 class A
  set cos 3
  exit
 class B
  exit

#show policy-map type queuing

Type queuing policy-maps
========================

policy-map type queuing default asd
 class type queuing default q0
  priority level 0
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
 class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 0
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
```

```
  exit
 class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit


#show policy-map interface xe1 statistics
Type qos class-map statistics:
+-----------+------------+-------------+--------------+---------------+
| Class-map | Match pkts | Match bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
 A            309283138   463924690500      -                -

Type queuing class-map statistics:
+-----------+------------+-------------+--------------+---------------+
| Class-map | Total pkts | Total bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+

#show policy-map interface xe1 statistics type qos
+-----------+------------+-------------+--------------+---------------+
| Class-map | Match pkts | Match bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
 A            310170136   465255187500      -                -

#show policy-map interface xe2 statistics type queuing
+-----------+------------+-------------+--------------+---------------+
| Class-map | Total pkts | Total bytes | Dropped pkts | Dropped Bytes |
+-----------+------------+-------------+--------------+---------------+
 q3          310941744    466412623500  12221          18331500
#
```

show policy-map interface

Use this command to:

1. Display non zero QoS statistics and configurations of type QOS and queuing policy-maps on an interface
2. Display the interfaces and policy-maps attached on them

Note: Queuing policy map drop statistics include all drop packets count in the queue (even policer drops).

Note: In order to check statistics, QoS statistics profile needs to be enabled for Qumran devices. QoS can either use ingress-acl statistics profile or ingress-qos statistics profile. When ACL groups are configured on the same interface as QoS and both ACL and QoS need explicit counters, then ingress-qos statistics profile needs to be configured along with ingress-acl statistics profile. However, this will have other limitations on statistics profiles. Please refer hardware-profile statistics for more details.

Command Syntax

```
show policy-map interface (NAME (type (qos (input | output |)| queuing)|)|brief)
```

Parameters

NAME	Interface name.
type	QoS or queuing type
brief	brief policy interface.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#show policy-map interface xe1

Interface xe1
Type QoS statistics status : enabled

Service-policy (qos) input: A
-----------------------------
Class-map (qos): A (match all)
 match vlan 2
 set cos 3
      matched      : 88091758 packets, 132137620500 bytes
      transmitted  : 88091758 packets, 132137620500 bytes

Class-map (qos): B (match all)
 match vlan 3


Service-policy (queuing) output: default-out-policy
---------------------------------
Class-map (queuing): q0
  priority level 0
```

```
Class-map (queuing): q1
  priority level 1

Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5

Class-map (queuing): q6
  priority level 6

Class-map (queuing): q7
  priority level 7


#show policy-map interface xe2

Interface xe2
Type QoS statistics status : enabled

Service-policy (queuing) output: asd
---------------------------------
Class-map (queuing): q0
  priority level 0

Class-map (queuing): q1
  priority level 1

Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3
      Output
         Total        : 88331951 packets, 132497934000 bytes
         Green        : 88332412 packets, 132498622500 bytes
         Yellow       : 0 packets, 0 bytes
      Dropped
         Total        : 0 packets, 0 bytes
         Green        : 0 packets, 0 bytes
         Yellow       : 0 packets, 0 bytes
         Red          : 0 packets, 0 bytes

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5
```

```
Class-map (queuing): q6
  priority level 6

Class-map (queuing): q7
  priority level 7


#show policy-map interface xe1 type qos input

Interface xe1
Type QoS statistics status : enabled

Service-policy (qos) input: A
-----------------------------
Class-map (qos): A (match all)
 match vlan 2
 set cos 3
      matched      : 89779233 packets, 134668833000 bytes
      transmitted  : 89779233 packets, 134668833000 bytes

Class-map (qos): B (match all)
 match vlan 3

#show policy-map interface xe2 type queuing

Interface xe2
Type QoS statistics status : enabled

Service-policy (queuing) output: asd
------------------------------------
Class-map (queuing): q0
  priority level 0

Class-map (queuing): q1
  priority level 1

Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3
      Output
         Total        : 119883527 packets, 179825298000 bytes
         Green        : 119883992 packets, 179825995500 bytes
         Yellow       : 0 packets, 0 bytes
      Dropped
         Total        : 0 packets, 0 bytes
         Green        : 0 packets, 0 bytes
         Yellow       : 0 packets, 0 bytes
         Red          : 0 packets, 0 bytes

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5
```

```
Class-map (queuing): q6
  priority level 6

Class-map (queuing): q7
  priority level 7


#show policy-map interface br
+------------+------------+------------------+
|            |    QOS     |                  |
| Interface  |-----+------|QUEUE             |
|            |INPUT|OUTPUT|                  |
+------------+-----+------+------------------+
 ce49                      default-out-policy
 ce50                      default-out-policy
```

show qos-profile

Use this command to show the all configured QoS profiles configurations like type, name, maps configured except for the default maps, attached info (to how many interfaces it is attached) etc,

Command Syntax

```
show qos-profile (type (cos-to-queue | dscp-to-queue | queue-color-to-cos | dscp-
  to-dscp | dscp-to-exp)|)(NAME|)
```

Parameters

cos-to-queue	Profile for cos to queue map
dscp-to-queue	Profile for dscp to queue map
queue-color-to-cos	Profile for queue color to cos map
dscp-to-dscp	Profile for inDscp to outDscp map
dscp-to-exp	Profile for dscp to exp map
exp-to-queue	Profile for exp to queue map
NAME	Profile map name (maximum 32 characters)

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#show policy-map interface xe1

Interface xe1
Type QoS statistics status : enabled

Service-policy (qos) input: A
----------------------------
Class-map (qos): A (match all)
 match vlan 2
 set cos 3
      matched      : 88091758 packets, 132137620500 bytes
      transmitted  : 88091758 packets, 132137620500 bytes

Class-map (qos): B (match all)
 match vlan 3


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
  priority level 0
```

```
Class-map (queuing): q1
  priority level 1
Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5

Class-map (queuing): q6
  priority level 6

Class-map (queuing): q7
  priority level 7


#show policy-map interface xe2

Interface xe2
Type QoS statistics status : enabled

Service-policy (queuing) output: asd
-----------------------------------
Class-map (queuing): q0
  priority level 0

Class-map (queuing): q1
  priority level 1

Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3
      Output
         Total        : 88331951 packets, 132497934000 bytes
         Green        : 88332412 packets, 132498622500 bytes
         Yellow       : 0 packets, 0 bytes
      Dropped
         Total        : 0 packets, 0 bytes
         Green        : 0 packets, 0 bytes
         Yellow       : 0 packets, 0 bytes
         Red          : 0 packets, 0 bytes

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5

Class-map (queuing): q6
  priority level 6
```

```
Class-map (queuing): q7
  priority level 7

#show policy-map interface xe1 type qos input

Interface xe1
Type QoS statistics status : enabled

Service-policy (qos) input: A
-----------------------------
Class-map (qos): A (match all)
 match vlan 2
 set cos 3
      matched      : 89779233 packets, 134668833000 bytes
      transmitted  : 89779233 packets, 134668833000 bytes

Class-map (qos): B (match all)
 match vlan 3

#show policy-map interface xe2 type queuing

Interface xe2
Type QoS statistics status : enabled

Service-policy (queuing) output: asd
-----------------------------------
Class-map (queuing): q0
  priority level 0

Class-map (queuing): q1
  priority level 1

Class-map (queuing): q2
  priority level 2

Class-map (queuing): q3
  priority level 3
      Output
         Total        : 119883527 packets, 179825298000 bytes
         Green        : 119883992 packets, 179825995500 bytes
         Yellow       : 0 packets, 0 bytes
      Dropped
         Total        : 0 packets, 0 bytes
         Green        : 0 packets, 0 bytes
         Yellow       : 0 packets, 0 bytes
         Red          : 0 packets, 0 bytes

Class-map (queuing): q4
  priority level 4

Class-map (queuing): q5
  priority level 5

Class-map (queuing): q6
  priority level 6
```

```
Class-map (queuing): q7
  priority level 7

#show policy-map interface br
+------------+------------+------------------+
|            |    QOS     |                  |
| Interface  |-----+------|QUEUE             |
|            |INPUT|OUTPUT|                  |
+------------+-----+------+------------------+
 ce49                      default-out-policy
 ce50                      default-out-policy
```

show qos-profile interface

Use this command to show the all configured QoS profiles configurations attached on an interface.

Command Syntax

```
show qos-profile interface NAME
```

Parameters

NAME	Profile map name (maximum 32 characters)

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#show qos-profile interface xe11
 profile name: cos-map
 profile type: cos-to-queue
 mapping:
 qos profile cos-to-queue cos-map
 cos 0 dei 0 queue 0 color green
 cos 0 dei 1 queue 0 color yellow
 cos 0 queue 0
 cos 1 dei 0 queue 1 color green
 cos 1 dei 1 queue 1 color yellow
 cos 1 queue 1
 cos 2 dei 0 queue 2 color green
 cos 2 dei 1 queue 2 color yellow
 cos 2 queue 2
 cos 3 dei 0 queue 3 color green
 cos 3 dei 1 queue 3 color yellow
 cos 3 queue 3
 cos 4 dei 0 queue 4 color green
 cos 4 dei 1 queue 4 color yellow
 cos 4 queue 4
 cos 5 dei 0 queue 5 color green
 cos 5 dei 1 queue 5 color yellow
 cos 5 queue 5
 cos 6 dei 0 queue 6 color green
```

show queuing interface

Use this command to see the configurations of queues that are attached to an interface.

Command Syntax

```
show queuing interface NAME
```

Parameters

NAME	Interface name.

Command Mode

Exec & config mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
# show queuing interface xe1/1
Egress Queuing for Ethernet xe1/1 [System]
------------------------------------------------------------------------------
----------------------
L0              L1              L2              Group PrioLevel   Shape
Bandwidth
------------------------------------------------------------------------------
----------------------
q0                                                      -      High        -
-
q1                                                      -      High        -
-
q2                                                      -      High        -
-
q3                                                      -      High        -
-
q4                                                      -      High        -
-
q5                                                      -      High        -
-
q6                                                      -      High        -
-
q7                                                      -      High        -
-
```

show running-config qos

Use this command to show the user configured QoS configurations.

Command Syntax

```
show running-config qos (all|)
```

Parameters

`all`	Show all QoS related configuration information including all defaults.

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#show running-config qos
qos enable
!
!
#show running-config qos  ?
  all  diplay all qos info including defaults
  |    Output modifiers
  >    Output redirection
  <cr>

#show running-config qos  all
qos enable
!
qos profile cos-to-queue default
 cos 0 dei 0 queue 0 color green
 cos 0 dei 1 queue 0 color yellow
 cos 0 queue 0
 cos 1 dei 0 queue 1 color green
 cos 1 dei 1 queue 1 color yellow
 cos 1 queue 1
 cos 2 dei 0 queue 2 color green
 cos 2 dei 1 queue 2 color yellow
 cos 2 queue 2
 cos 3 dei 0 queue 3 color green
 cos 3 dei 1 queue 3 color yellow
 cos 3 queue 3
 cos 4 dei 0 queue 4 color green
 cos 4 dei 1 queue 4 color yellow
 cos 4 queue 4
 cos 5 dei 0 queue 5 color green
 cos 5 dei 1 queue 5 color yellow
 cos 5 queue 5
 cos 6 dei 0 queue 6 color green
 cos 6 dei 1 queue 6 color yellow
 cos 6 queue 6
```

```
 cos 7 dei 0 queue 7 color green
 cos 7 dei 1 queue 7 color yellow
 cos 7 queue 7
!
qos profile queue-color-to-cos default
 queue 0 color green cos 0
 queue 0 color yellow cos 0
 queue 0 color red cos 0
 queue 0 cos 0
 queue 1 color green cos 1
 queue 1 color yellow cos 1
 queue 1 color red cos 1
 queue 1 cos 1
 queue 2 color green cos 2
 queue 2 color yellow cos 2
 queue 2 color red cos 2
 queue 2 cos 2
 queue 3 color green cos 3
 queue 3 color yellow cos 3
 queue 3 color red cos 3
 queue 3 cos 3
 queue 4 color green cos 4
 queue 4 color yellow cos 4
 queue 4 color red cos 4
 queue 4 cos 4
 queue 5 color green cos 5
 queue 5 color yellow cos 5
 queue 5 color red cos 5
 queue 5 cos 5
 queue 6 color green cos 6
 queue 6 color yellow cos 6
 queue 6 color red cos 6
 queue 6 cos 6
 queue 7 color green cos 7
 queue 7 color yellow cos 7
 queue 7 color red cos 7
 queue 7 cos 7
!
qos profile dscp-to-queue default
 dscp 0 queue 0 color green dscp 0
 dscp 1 queue 0 color green dscp 1
 dscp 2 queue 0 color green dscp 2
 dscp 3 queue 0 color green dscp 3
 dscp 4 queue 0 color green dscp 4
 dscp 5 queue 0 color green dscp 5
 dscp 6 queue 0 color green dscp 6
 dscp 7 queue 0 color green dscp 7
 dscp 8 queue 1 color green dscp 8
 dscp 9 queue 1 color green dscp 9
 dscp 10 queue 1 color green dscp 10
 dscp 11 queue 1 color green dscp 11
 dscp 12 queue 1 color yellow dscp 12
 dscp 13 queue 1 color green dscp 13
 dscp 14 queue 1 color yellow dscp 14
 dscp 15 queue 1 color green dscp 15
 dscp 16 queue 2 color green dscp 16
 dscp 17 queue 2 color green dscp 17
```

```
 dscp 18 queue 2 color green dscp 18
 dscp 19 queue 2 color green dscp 19
 dscp 20 queue 2 color yellow dscp 20
 dscp 21 queue 2 color green dscp 21
 dscp 22 queue 2 color yellow dscp 22
 dscp 23 queue 2 color green dscp 23
 dscp 24 queue 3 color green dscp 24
 dscp 25 queue 3 color green dscp 25
 dscp 26 queue 3 color green dscp 26
 dscp 27 queue 3 color green dscp 27
 dscp 28 queue 3 color yellow dscp 28
 dscp 29 queue 3 color green dscp 29
 dscp 30 queue 3 color yellow dscp 30
 dscp 31 queue 3 color green dscp 31
 dscp 32 queue 4 color green dscp 32
 dscp 33 queue 4 color green dscp 33
 dscp 34 queue 4 color green dscp 34
 dscp 35 queue 4 color green dscp 35
 dscp 36 queue 4 color yellow dscp 36
 dscp 37 queue 4 color green dscp 37
 dscp 38 queue 4 color yellow dscp 38
 dscp 39 queue 4 color green dscp 39
 dscp 40 queue 5 color green dscp 40
 dscp 41 queue 5 color green dscp 41
 dscp 42 queue 5 color green dscp 42
 dscp 43 queue 5 color green dscp 43
 dscp 44 queue 5 color green dscp 44
 dscp 45 queue 5 color green dscp 45
 dscp 46 queue 5 color green dscp 46
 dscp 47 queue 5 color green dscp 47
 dscp 48 queue 6 color green dscp 48
 dscp 49 queue 6 color green dscp 49
 dscp 50 queue 6 color green dscp 50
 dscp 51 queue 6 color green dscp 51
 dscp 52 queue 6 color green dscp 52
 dscp 53 queue 6 color green dscp 53
 dscp 54 queue 6 color green dscp 54
 dscp 55 queue 6 color green dscp 55
 dscp 56 queue 7 color green dscp 56
 dscp 57 queue 7 color green dscp 57
 dscp 58 queue 7 color green dscp 58
 dscp 59 queue 7 color green dscp 59
 dscp 60 queue 7 color green dscp 60
 dscp 61 queue 7 color green dscp 61
 dscp 62 queue 7 color green dscp 62
 dscp 63 queue 7 color green dscp 63
!
qos profile dscp-to-dscp default
 dscp 0 color green dscp 0
 dscp 0 color yellow dscp 0
 dscp 0 color red dscp 0
 dscp 0 dscp 0
 dscp 1 color green dscp 1
 dscp 1 color yellow dscp 1
 dscp 1 color red dscp 1
 dscp 1 dscp 1
 dscp 2 color green dscp 2
```

```
dscp 2 color yellow dscp 2
dscp 2 color red dscp 2
dscp 2 dscp 2
dscp 3 color green dscp 3
dscp 3 color yellow dscp 3
dscp 3 color red dscp 3
dscp 3 dscp 3
dscp 4 color green dscp 4
dscp 4 color yellow dscp 4
dscp 4 color red dscp 4
dscp 4 dscp 4
dscp 5 color green dscp 5
dscp 5 color yellow dscp 5
dscp 5 color red dscp 5
dscp 5 dscp 5
dscp 6 color green dscp 6
dscp 6 color yellow dscp 6
dscp 6 color red dscp 6
dscp 6 dscp 6
dscp 7 color green dscp 7
dscp 7 color yellow dscp 7
dscp 7 color red dscp 7
dscp 7 dscp 7
dscp 8 color green dscp 8
dscp 8 color yellow dscp 8
dscp 8 color red dscp 8
dscp 8 dscp 8
dscp 9 color green dscp 9
dscp 9 color yellow dscp 9
dscp 9 color red dscp 9
dscp 9 dscp 9
dscp 10 color green dscp 10
dscp 10 color yellow dscp 10
dscp 10 color red dscp 10
dscp 10 dscp 10
dscp 11 color green dscp 11
dscp 11 color yellow dscp 11
dscp 11 color red dscp 11
dscp 11 dscp 11
dscp 12 color green dscp 12
dscp 12 color yellow dscp 12
dscp 12 color red dscp 12
dscp 12 dscp 12
dscp 13 color green dscp 13
dscp 13 color yellow dscp 13
dscp 13 color red dscp 13
dscp 13 dscp 13
dscp 14 color green dscp 14
dscp 14 color yellow dscp 14
dscp 14 color red dscp 14
dscp 14 dscp 14
dscp 15 color green dscp 15
dscp 15 color yellow dscp 15
dscp 15 color red dscp 15
dscp 15 dscp 15
dscp 16 color green dscp 16
dscp 16 color yellow dscp 16
```

```
dscp 16 color red dscp 16
dscp 16 dscp 16
dscp 17 color green dscp 17
dscp 17 color yellow dscp 17
dscp 17 color red dscp 17
dscp 17 dscp 17
dscp 18 color green dscp 18
dscp 18 color yellow dscp 18
dscp 18 color red dscp 18
dscp 18 dscp 18
dscp 19 color green dscp 19
dscp 19 color yellow dscp 19
dscp 19 color red dscp 19
dscp 19 dscp 19
dscp 20 color green dscp 20
dscp 20 color yellow dscp 20
dscp 20 color red dscp 20
dscp 20 dscp 20
dscp 21 color green dscp 21
dscp 21 color yellow dscp 21
dscp 21 color red dscp 21
dscp 21 dscp 21
dscp 22 color green dscp 22
dscp 22 color yellow dscp 22
dscp 22 color red dscp 22
dscp 22 dscp 22
dscp 23 color green dscp 23
dscp 23 color yellow dscp 23
dscp 23 color red dscp 23
dscp 23 dscp 23
dscp 24 color green dscp 24
dscp 24 color yellow dscp 24
dscp 24 color red dscp 24
dscp 24 dscp 24
dscp 25 color green dscp 25
dscp 25 color yellow dscp 25
dscp 25 color red dscp 25
dscp 25 dscp 25
dscp 26 color green dscp 26
dscp 26 color yellow dscp 26
dscp 26 color red dscp 26
dscp 26 dscp 26
dscp 27 color green dscp 27
dscp 27 color yellow dscp 27
dscp 27 color red dscp 27
dscp 27 dscp 27
dscp 28 color green dscp 28
dscp 28 color yellow dscp 28
dscp 28 color red dscp 28
dscp 28 dscp 28
dscp 29 color green dscp 29
dscp 29 color yellow dscp 29
dscp 29 color red dscp 29
dscp 29 dscp 29
dscp 30 color green dscp 30
dscp 30 color yellow dscp 30
dscp 30 color red dscp 30
```

```
dscp 30 dscp 30
dscp 31 color green dscp 31
dscp 31 color yellow dscp 31
dscp 31 color red dscp 31
dscp 31 dscp 31
dscp 32 color green dscp 32
dscp 32 color yellow dscp 32
dscp 32 color red dscp 32
dscp 32 dscp 32
dscp 33 color green dscp 33
dscp 33 color yellow dscp 33
dscp 33 color red dscp 33
dscp 33 dscp 33
dscp 34 color green dscp 34
dscp 34 color yellow dscp 34
dscp 34 color red dscp 34
dscp 34 dscp 34
dscp 35 color green dscp 35
dscp 35 color yellow dscp 35
dscp 35 color red dscp 35
dscp 35 dscp 35
dscp 36 color green dscp 36
dscp 36 color yellow dscp 36
dscp 36 color red dscp 36
dscp 36 dscp 36
dscp 37 color green dscp 37
dscp 37 color yellow dscp 37
dscp 37 color red dscp 37
dscp 37 dscp 37
dscp 38 color green dscp 38
dscp 38 color yellow dscp 38
dscp 38 color red dscp 38
dscp 38 dscp 38
dscp 39 color green dscp 39
dscp 39 color yellow dscp 39
dscp 39 color red dscp 39
dscp 39 dscp 39
dscp 40 color green dscp 40
dscp 40 color yellow dscp 40
dscp 40 color red dscp 40
dscp 40 dscp 40
dscp 41 color green dscp 41
dscp 41 color yellow dscp 41
dscp 41 color red dscp 41
dscp 41 dscp 41
dscp 42 color green dscp 42
dscp 42 color yellow dscp 42
dscp 42 color red dscp 42
dscp 42 dscp 42
dscp 43 color green dscp 43
dscp 43 color yellow dscp 43
dscp 43 color red dscp 43
dscp 43 dscp 43
dscp 44 color green dscp 44
dscp 44 color yellow dscp 44
dscp 44 color red dscp 44
dscp 44 dscp 44
```

```
dscp 45 color green dscp 45
dscp 45 color yellow dscp 45
dscp 45 color red dscp 45
dscp 45 dscp 45
dscp 46 color green dscp 46
dscp 46 color yellow dscp 46
dscp 46 color red dscp 46
dscp 46 dscp 46
dscp 47 color green dscp 47
dscp 47 color yellow dscp 47
dscp 47 color red dscp 47
dscp 47 dscp 47
dscp 48 color green dscp 48
dscp 48 color yellow dscp 48
dscp 48 color red dscp 48
dscp 48 dscp 48
dscp 49 color green dscp 49
dscp 49 color yellow dscp 49
dscp 49 color red dscp 49
dscp 49 dscp 49
dscp 50 color green dscp 50
dscp 50 color yellow dscp 50
dscp 50 color red dscp 50
dscp 50 dscp 50
dscp 51 color green dscp 51
dscp 51 color yellow dscp 51
dscp 51 color red dscp 51
dscp 51 dscp 51
dscp 52 color green dscp 52
dscp 52 color yellow dscp 52
dscp 52 color red dscp 52
dscp 52 dscp 52
dscp 53 color green dscp 53
dscp 53 color yellow dscp 53
dscp 53 color red dscp 53
dscp 53 dscp 53
dscp 54 color green dscp 54
dscp 54 color yellow dscp 54
dscp 54 color red dscp 54
dscp 54 dscp 54
dscp 55 color green dscp 55
dscp 55 color yellow dscp 55
dscp 55 color red dscp 55
dscp 55 dscp 55
dscp 56 color green dscp 56
dscp 56 color yellow dscp 56
dscp 56 color red dscp 56
dscp 56 dscp 56
dscp 57 color green dscp 57
dscp 57 color yellow dscp 57
dscp 57 color red dscp 57
dscp 57 dscp 57
dscp 58 color green dscp 58
dscp 58 color yellow dscp 58
dscp 58 color red dscp 58
dscp 58 dscp 58
dscp 59 color green dscp 59
```

```
 dscp 59 color yellow dscp 59
 dscp 59 color red dscp 59
 dscp 59 dscp 59
 dscp 60 color green dscp 60
 dscp 60 color yellow dscp 60
 dscp 60 color red dscp 60
 dscp 60 dscp 60
 dscp 61 color green dscp 61
dscp 61 color yellow dscp 61
 dscp 61 color red dscp 61
 dscp 61 dscp 61
 dscp 62 color green dscp 62
 dscp 62 color yellow dscp 62
 dscp 62 color red dscp 62
 dscp 62 dscp 62
 dscp 63 color green dscp 63
 dscp 63 color yellow dscp 63
 dscp 63 color red dscp 63
 dscp 63 dscp 63
!
qos profile exp-to-queue default
 exp 0 queue 0 color green
 exp 1 queue 1 color green
 exp 2 queue 2 color green
 exp 3 queue 3 color green
 exp 4 queue 4 color green
 exp 5 queue 5 color green
 exp 6 queue 6 color green
 exp 7 queue 7 color green
!
qos profile dscp-to-exp default
 dscp 0 color green exp 0
 dscp 0 color yellow exp 0
 dscp 0 color red exp 0
 dscp 0 exp 0
 dscp 1 color green exp 0
 dscp 1 color yellow exp 0
 dscp 1 color red exp 0
 dscp 1 exp 0
 dscp 2 color green exp 0
 dscp 2 color yellow exp 0
 dscp 2 color red exp 0
 dscp 2 exp 0
 dscp 3 color green exp 0
 dscp 3 color yellow exp 0
 dscp 3 color red exp 0
 dscp 3 exp 0
 dscp 4 color green exp 0
 dscp 4 color yellow exp 0
 dscp 4 color red exp 0
 dscp 4 exp 0
 dscp 5 color green exp 0
 dscp 5 color yellow exp 0
 dscp 5 color red exp 0
 dscp 5 exp 0
 dscp 6 color green exp 0
 dscp 6 color yellow exp 0
```



```
dscp 6 color red exp 0
dscp 6 exp 0
dscp 7 color green exp 0
dscp 7 color yellow exp 0
dscp 7 color red exp 0
dscp 7 exp 0
dscp 8 color green exp 1
dscp 8 color yellow exp 1
dscp 8 color red exp 1
dscp 8 exp 1
dscp 9 color green exp 1
dscp 9 color yellow exp 1
dscp 9 color red exp 1
dscp 9 exp 1
dscp 10 color green exp 1
dscp 10 color yellow exp 1
dscp 10 color red exp 1
dscp 10 exp 1
dscp 11 color green exp 1
dscp 11 color yellow exp 1
dscp 11 color red exp 1
dscp 11 exp 1
dscp 12 color green exp 1
dscp 12 color yellow exp 1
dscp 12 color red exp 1
dscp 12 exp 1
dscp 13 color green exp 1
dscp 13 color yellow exp 1
dscp 13 color red exp 1
dscp 13 exp 1
dscp 14 color green exp 1
dscp 14 color yellow exp 1
dscp 14 color red exp 1
dscp 14 exp 1
dscp 15 color green exp 1
dscp 15 color yellow exp 1
dscp 15 color red exp 1
dscp 15 exp 1
dscp 16 color green exp 2
dscp 16 color yellow exp 2
dscp 16 color red exp 2
dscp 16 exp 2
dscp 17 color green exp 2
dscp 17 color yellow exp 2
dscp 17 color red exp 2
dscp 17 exp 2
dscp 18 color green exp 2
dscp 18 color yellow exp 2
dscp 18 color red exp 2
dscp 18 exp 2
dscp 19 color green exp 2
dscp 19 color yellow exp 2
dscp 19 color red exp 2
dscp 19 exp 2
dscp 20 color green exp 2
dscp 20 color yellow exp 2
dscp 20 color red exp 2
```

```
dscp 20 exp 2
dscp 21 color green exp 2
dscp 21 color yellow exp 2
dscp 21 color red exp 2
dscp 21 exp 2
dscp 22 color green exp 2
dscp 22 color yellow exp 2
dscp 22 color red exp 2
dscp 22 exp 2
dscp 23 color green exp 2
dscp 23 color yellow exp 2
dscp 23 color red exp 2
dscp 23 exp 2
dscp 24 color green exp 3
dscp 24 color yellow exp 3
dscp 24 color red exp 3
dscp 24 exp 3
dscp 25 color green exp 3
dscp 25 color yellow exp 3
dscp 25 color red exp 3
dscp 25 exp 3
dscp 26 color green exp 3
dscp 26 color yellow exp 3
dscp 26 color red exp 3
dscp 26 exp 3
dscp 27 color green exp 3
dscp 27 color yellow exp 3
dscp 27 color red exp 3
dscp 27 exp 3
dscp 28 color green exp 3
dscp 28 color yellow exp 3
dscp 28 color red exp 3
dscp 28 exp 3
dscp 29 color green exp 3
dscp 29 color yellow exp 3
dscp 29 color red exp 3
dscp 29 exp 3
dscp 30 color green exp 3
dscp 30 color yellow exp 3
dscp 30 color red exp 3
dscp 30 exp 3
dscp 31 color green exp 3
dscp 31 color yellow exp 3
dscp 31 color red exp 3
dscp 31 exp 3
dscp 32 color green exp 4
dscp 32 color yellow exp 4
dscp 32 color red exp 4
dscp 32 exp 4
dscp 33 color green exp 4
dscp 33 color yellow exp 4
dscp 33 color red exp 4
dscp 33 exp 4
dscp 34 color green exp 4
dscp 34 color yellow exp 4
dscp 34 color red exp 4
dscp 34 exp 4
```

```
dscp 35 color green exp 4
dscp 35 color yellow exp 4
dscp 35 color red exp 4
dscp 35 exp 4
dscp 36 color green exp 4
dscp 36 color yellow exp 4
dscp 36 color red exp 4
dscp 36 exp 4
dscp 37 color green exp 4
dscp 37 color yellow exp 4
dscp 37 color red exp 4
dscp 37 exp 4
dscp 38 color green exp 4
dscp 38 color yellow exp 4
dscp 38 color red exp 4
dscp 38 exp 4
dscp 39 color green exp 4
dscp 39 color yellow exp 4
dscp 39 color red exp 4
dscp 39 exp 4
dscp 40 color green exp 5
dscp 40 color yellow exp 5
dscp 40 color red exp 5
dscp 40 exp 5
dscp 41 color green exp 5
dscp 41 color yellow exp 5
dscp 41 color red exp 5
dscp 41 exp 5
dscp 42 color green exp 5
dscp 42 color yellow exp 5
dscp 42 color red exp 5
dscp 42 exp 5
dscp 43 color green exp 5
dscp 43 color yellow exp 5
dscp 43 color red exp 5
dscp 43 exp 5
dscp 44 color green exp 5
dscp 44 color yellow exp 5
dscp 44 color red exp 5
dscp 44 exp 5
dscp 45 color green exp 5
dscp 45 color yellow exp 5
dscp 45 color red exp 5
dscp 45 exp 5
dscp 46 color green exp 5
dscp 46 color yellow exp 5
dscp 46 color red exp 5
dscp 46 exp 5
dscp 47 color green exp 5
dscp 47 color yellow exp 5
dscp 47 color red exp 5
dscp 47 exp 5
dscp 48 color green exp 6
dscp 48 color yellow exp 6
dscp 48 color red exp 6
dscp 48 exp 6
dscp 49 color green exp 6
```

```
dscp 49 color yellow exp 6
dscp 49 color red exp 6
dscp 49 exp 6
dscp 50 color green exp 6
dscp 50 color yellow exp 6
dscp 50 color red exp 6
dscp 50 exp 6
dscp 51 color green exp 6
dscp 51 color yellow exp 6
dscp 51 color red exp 6
dscp 51 exp 6
dscp 52 color green exp 6
dscp 52 color yellow exp 6
dscp 52 color red exp 6
dscp 52 exp 6
dscp 53 color green exp 6
dscp 53 color yellow exp 6
dscp 53 color red exp 6
dscp 53 exp 6
dscp 54 color green exp 6
dscp 54 color yellow exp 6
dscp 54 color red exp 6
dscp 54 exp 6
dscp 55 color green exp 6
dscp 55 color yellow exp 6
dscp 55 color red exp 6
dscp 55 exp 6
dscp 56 color green exp 7
dscp 56 color yellow exp 7
dscp 56 color red exp 7
dscp 56 exp 7
dscp 57 color green exp 7
dscp 57 color yellow exp 7
dscp 57 color red exp 7
dscp 57 exp 7
dscp 58 color green exp 7
dscp 58 color yellow exp 7
dscp 58 color red exp 7
dscp 58 exp 7
dscp 59 color green exp 7
dscp 59 color yellow exp 7
dscp 59 color red exp 7
dscp 59 exp 7
dscp 60 color green exp 7
dscp 60 color yellow exp 7
dscp 60 color red exp 7
dscp 60 exp 7
dscp 61 color green exp 7
dscp 61 color yellow exp 7
dscp 61 color red exp 7
dscp 61 exp 7
dscp 62 color green exp 7
dscp 62 color yellow exp 7
dscp 62 color red exp 7
dscp 62 exp 7
dscp 63 color green exp 7
dscp 63 color yellow exp 7
```

```
 dscp 63 color red exp 7
 dscp 63 exp 7
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 0
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 2
  exit
 class type queuing default q3
  priority level 3
  exit
 class type queuing default q4
  priority level 4
  exit
 class type queuing default q5
  priority level 5
  exit
class type queuing default q6
  priority level 6
  exit
 class type queuing default q7
  priority level 7
  exit
!
interface ce49
 service-policy type queuing output default-out-policy
!
interface ce50
 service-policy type queuing output default-out-policy
!
interface ce51
 service-policy type queuing output default-out-policy
!
interface ce52
 service-policy type queuing output default-out-policy
!
interface ce53
 service-policy type queuing output default-out-policy
!
interface ce54
 service-policy type queuing output default-out-policy
!
interface xe1
 service-policy type queuing output default-out-policy
!
interface xe2
 service-policy type queuing output default-out-policy
!
interface xe3
 service-policy type queuing output default-out-policy
!
interface xe4
```

```
 service-policy type queuing output default-out-policy
!
interface xe5
 service-policy type queuing output default-out-policy
!
interface xe6
 service-policy type queuing output default-out-policy
!
interface xe7
 service-policy type queuing output default-out-policy
!
interface xe8
 service-policy type queuing output default-out-policy
!
interface xe9
 service-policy type queuing output default-out-policy
!
interface xe10
 service-policy type queuing output default-out-policy
!
interface xe11
 service-policy type queuing output default-out-policy
!
interface xe12
 service-policy type queuing output default-out-policy
!
interface xe13
 service-policy type queuing output default-out-policy
!
interface xe14
 service-policy type queuing output default-out-policy
!
interface xe15
 service-policy type queuing output default-out-policy
!
interface xe16
 service-policy type queuing output default-out-policy
!
interface xe17
 service-policy type queuing output default-out-policy
!
interface xe18
 service-policy type queuing output default-out-policy
!
interface xe19
 service-policy type queuing output default-out-policy
!
interface xe20
 service-policy type queuing output default-out-policy
!
interface xe21
 service-policy type queuing output default-out-policy
!
interface xe22
 service-policy type queuing output default-out-policy
!
interface xe23
```



```
service-policy type queuing output default-out-policy
!
interface xe24
 service-policy type queuing output default-out-policy
!
interface xe25
 service-policy type queuing output default-out-policy
!
interface xe26
 service-policy type queuing output default-out-policy
!
interface xe27
 service-policy type queuing output default-out-policy
!
interface xe28
 service-policy type queuing output default-out-policy
!
interface xe29
 service-policy type queuing output default-out-policy
!
interface xe30
 service-policy type queuing output default-out-policy
!
interface xe31
 service-policy type queuing output default-out-policy
!
interface xe32
 service-policy type queuing output default-out-policy
!
interface xe33
 service-policy type queuing output default-out-policy
!
interface xe34
 service-policy type queuing output default-out-policy
!
interface xe35
 service-policy type queuing output default-out-policy
!
interface xe36
 service-policy type queuing output default-out-policy
!
interface xe37
 service-policy type queuing output default-out-policy
!
interface xe38
 service-policy type queuing output default-out-policy
!
interface xe39
 service-policy type queuing output default-out-policy
!
interface xe40
 service-policy type queuing output default-out-policy
!
interface xe41
 service-policy type queuing output default-out-policy
!
interface xe42
```

```
 service-policy type queuing output default-out-policy
!
interface xe43
 service-policy type queuing output default-out-policy
!
interface xe44
 service-policy type queuing output default-out-policy
!
interface xe45
 service-policy type queuing output default-out-policy
!
interface xe46
service-policy type queuing output default-out-policy
!
interface xe47
 service-policy type queuing output default-out-policy
!
interface xe48
 service-policy type queuing output default-out-policy
!
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

The minimum granularity for storm-control is 64kbps.

Use the no form of this command to disable storm control.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
  (kbps|mbps|gbps))
no storm-control (broadcast|multicast|dlf)
```

Parameters

broadcast	Broadcast rate limiting.
multicast	Multicast rate limiting.
dlf	Destination lookup failure limiting.
level	Sets the percentage of the threshold.
LEVEL	The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.
<0-1000000000>	Sets absolute threshold value <0-1000000000>
kbps	specifies the units of Kilobits per second.
mbps	specifies the units of Megabits per second.
gbps	specifies the units of Gigabits per second.

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#storm-control broadcast level 30

(config)#interface xe2
(config-if)#storm-control multicast level 30
```

```
(config)#interface xe3
(config-if)#storm-control multicast 300 mbps

(config)#interface xe4
(config-if)#no storm-control multicast
```

tust dscp

Use this command to classify the traffic based on dscp map on L2 port.

Use the no form of the command to remove the configuration.

Note: By default, the trust of L2 ports is CoS. If the user wants to map the traffic according to the DSCP value, `trust dscp` can be set on ports to achieve the requirement.

Tagged packet color is based on the DEI bit. Untagged packet color is based on DSCP value.

Out-DSCP option in dscp-to-queue profile is not applicable on L2 interfaces when trust DSCP is set

Only “default” dscp-to-queue profile is valid for trust DSCP. User-defined `dscp-to-queue` cannot be attached on L2 interfaces.

Command Syntax

```
trust dscp
no trust dscp
```

Parameters

`trust`	Configure port trust state
`dscp`	Classifies ingress packets with the packet DSCP values

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#interface xe1
(config-if)#trust dscp
```

wfq-queue weight

Use this command to set WFQ-queue weight for a queue.

Use the no form of the command to un-set configured WFQ configuration.

Command Syntax

```
wfq-queue weight <1-127>
no wfq-queue weights
```

Parameters

<1-127>	WFQ queue weight to be configured.

Default

No default value is specified

Command Mode

Policy-class-map queuing Mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#policy-map type queuing default default-out-policy
(config-pmap-que-def)# class type queuing default q0
(config-pmap-c-que-def)#wfq-queue weight 2
```

vc-qos map-profile

Use this command is used to binding PCP to TC mapping profile to attachment circuits.

Use the no form of this command to remove the profile.

Note: Profile configured on the VPLS service is effective for all attachment circuits associated with VPLS service. However, if a profile is bound to attachment circuit, that profile takes higher priority for that attachment circuit.

Command Syntax

```
vc-qos map-profile (cos-to-queue | queue-color-to-cos) NAME
no vc-qos map-profile (cos-to-queue | queue-color-to-cos)  NAME
```

Parameters

cos-to-queue	Profile for cos to queue map
queue-color-to-cos	Profile for queue-color to cos map
NAME	Profile map name (maximum 32 characters)

Default

By-default, “default” global cos-to-queue map is applied on an attachment-circuit if no user-defined cos-to-queue profile is applied on interface or vpls-service.

Traffic received on VPLS service will be affected by QoS treatment by configurations in the following order:

1. PCP to TC/TC to PCP profile configuration bound to attachment circuit.
2. PCP to TC/TC to PCP profile configuration bound to VPLS service.
3. PCP to TC/TC to PCP profile configuration bound to ingress port.
4. Global PCP to TC/TC to PCP profile configuration.

Command Mode

interface-vpls modes

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#interface xe1
(config-if)#switchport
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#vc-qos map-profile queue-color-to-cos qc-profile-2
```

vpls-qos map-profile

Use this command is used to binding PCP to TC mapping profile to VPLS service.

Use the no form of this command to remove the profile.

Command Syntax

```
vpls-qos map-profile (cos-to-queue | queue-color-to-cos) NAME
no vpls-qos map-profile (cos-to-queue | queue-color-to-cos) NAME
```

Parameters

`cos-to-queue`	Profile for cos to queue map
`queue-color-to-cos`	Profile for queue-color to cos map
`NAME`	Profile map name (maximum 32 characters)

Default

By-default, “default” global `cos-to-queue` map is applied on a VPLS service if no user-defined `cos-to-queue` profile is applied on interface.

Traffic received on a VPLS service will be affected by QoS treatment by configurations in the following order:

1. PCP to TC profile configuration bound to VPLS service.
2. PCP to TC profile configuration bound to ingress port.
3. Global PCP to TC profile configuration.

Command Mode

vpls modes

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#mpls vpls vpls1 1
(config-vpls)#vpls-qos map-profile cos-to-queue cq-profile-1
```

SECTION 16 Virtual eXtensible Local Area Network

Virtual eXtensible Local Area Network Configuration Guide

Contents

This guide contains the chapters:

CHAPTER 1 Overview

This chapter provides an overview of Virtual eXtensible Local Area Network (VXLAN) and its implementation with OcNOS. VXLAN creates LAN segments using a MAC in IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another server using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel EndPoints). This technology allows the network to support several tenants with minimum changes in the network. The VTEPs carry tenant data in L3 tunnels over the network. The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have the same IP or MAC addresses on end devices, hosts/VM's.

OcNOS supports VxLAN IPv4 tunnels, but both IPv4 and IPv6 hosts are supported.

Terminology

Terms related to VXLAN configuration are defined in the table below.

IGMP	Internet Group Management Protocol
PIM	Protocol Independent Multicast
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNI	VXLAN Network Identifier (or VXLAN Segment ID)
VTEP	VXLAN Tunnel End Point. An entity that originates and/or terminates VXLAN tunnels
VXLAN	Virtual eXtensible Local Area Network
VXLAN Segment	VXLAN Layer 2 overlay network over which VMs communicate
VXLAN Gateway	An entity that forwards traffic between VXLANs

VXLAN Architecture

VXLAN runs over the existing networking infrastructure. It provides a means to "stretch" a Layer 2 network. In short, VXLAN is a Layer 2 overlay scheme on a Layer 3 network.

Each overlay is termed as a VXLAN segment. Only VMs within the same VXLAN segment can communicate with each other. Each VXLAN segment is identified through a 24-bit segment ID termed the "VXLAN Network Identifier (VNI)". This allows up to 16 million VXLAN segments to coexist within the same administrative domain.

VNI identifies the scope of the inner MAC frame originated by the individual VM. Hence, we can have overlapping MAC addresses across segments but never have traffic "cross over" since the traffic is isolated using the VNI. The VNI is in an outer header that encapsulates the inner MAC frame originated by the VM.

Any packets (including ARP-ND) that are uplifted to the VxLAN CPU queue from any port are rate limited to 500 packets/second. This is done to protect the system and CPU during an ARP storm.

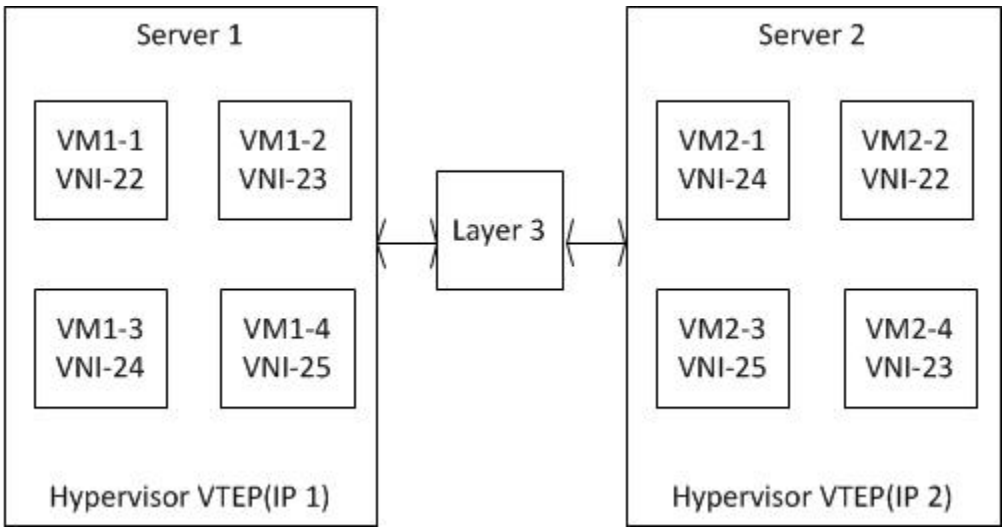


Figure 1-125: VXLAN Deployment - VTEPs across a Layer 3 Network

CHAPTER 2 VXLAN-EVPN Configuration

This section contains basic VXLAN-EVPN configuration examples.

VXLAN (Virtual eXtended LAN) creates LAN segments using a MAC-in-IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another host using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel End Points). The VTEPs carry tenant data in L3 tunnels over the network which permits the network to support multiple tenants.The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have same IP/MAC addresses.

Information about the given VM to get to the VTEP is crucial in VXLAN protocol; therefore BGP-MP is used to carry this information across VTEPS.

Note: For port-channel/Static-channel interface, storm control will be applied on each member port. For Example: if Interface eth1 and interface eth2 is part of port-channel i.e. po1 and storm control 2mbps is applied for broadcast traffic, then the storm control settings will be applied on each member port and broadcast traffic on each member port will be rate limited to 2mbps each.

Topology

The procedures in this section use the topology in Figure 2-126.

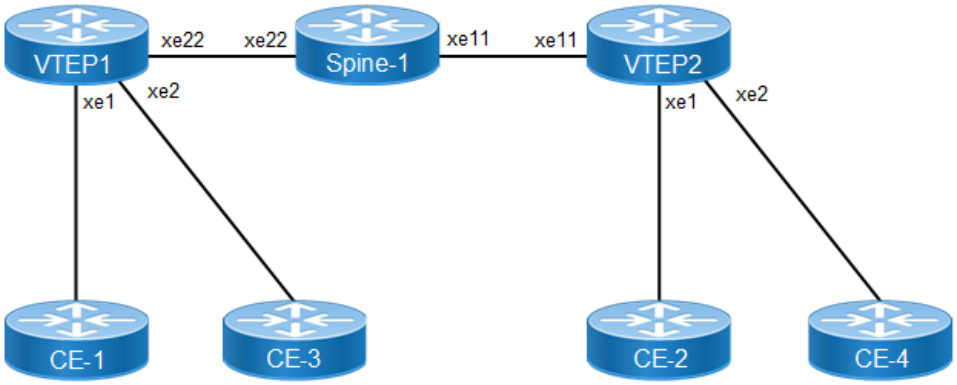


Figure 2-126: VXLAN EVPN

VTEP1

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#no shutdown`	Bring the interface into operation.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe22`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Set an IP address on the interface.

`(config-if)#no shutdown`	Bring the interface into operation.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set an IP address on the interface.
`(config-if)#no shutdown`	Bring the interface into operation.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance (ABC).
`(config-router)#is-type level-1`	Configure instance as level-1-only routing.
`(config-router)#net 49.0001.1111.1111.1111.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit router mode.
`(config)#interface xe22`	Enter interface mode
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface (ABC).
`(config-if)#isis circuit-type level-1`	Configure instance as level-1-only routing.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#isis circuit-type level-1`	Configure instance as level-1-only routing.
`(config-if)#exit`	Exit interface mode.
`(config)#mac vrf vrf_evpn_100`	Configure a new VRF named `vrf_evpn_100`.
`(config-vrf)#rd 1.1.1.1:1`	Assign the Route Distinguisher value.
`(config-vrf)#route-target both 100:1`	Configure route target to import and export the routes.
`(config-vrf)#exit`	Exit VRF mode.
`(config)#router bgp 1`	Define the routing process. The number 1 specifies the AS number of VTEP1.
`(config-router)#bgp router-id 1.1.1.1`	Configure router-id for this BGP process.
`(config-router)#neighbor 2.2.2.2 remote-as 1`	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 1 is the neighbor's AS number.
`(config-router)# neighbor 2.2.2.2 update-source 1.1.1.1`	Define BGP neighbor: 1.1.1.1 is the peer interface.
`(config-router)#address-family l2vpn evpn`	Configure address-family L2VPN EVPN.
`(config-router-af)#neighbor 2.2.2.2 activate`	Activate the neighbor in the EVPN address family.
`(config-router-af)#exit-address-family`	Exit the address-family mode.
`(config-router)#exit`	Exit router mode.
`(config)#hardware-profile filter vxlan enable`	Enable hardware-profile filter for VXLAN.
`(config)#nvo vxlan enable`	Enable VXLAN globally on this VTEP.
`(config)#nvo vxlan vtep-ip-global 1.1.1.1`	Assign a global IP to the VTEP.
`(config)#nvo vxlan id 100 ingress-replication`	Configure a VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf_evpn_100`.

(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe1 2	Configure access-port xe1 and map vlan 2
(config-nvo-acc-if)#map vnid 100	Map VNID 100 to access-port xe1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200 ingress-replication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with vrf_evpn_100
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe2 3	Configure access-port xe2 and map vlan 3
(config-nvo-acc-if)#map vnid 200	Map VNID 200 to access-port xe2.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

Spine-1

#configure terminal	Enter configure mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.3333.3333.3333.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP2

#configure terminal	Enter configure mode.
(config)#interface po1	Enter interface mode

`(config-if)#switchport`	Configure the interface as a switchport.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Set an IP address on the interface.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set an IP address on the interface.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance (ABC).
`(config-router)#is-type level-1`	Configure instance as level-1-only routing.
`(config-router)#net 49.0001.2222.2222.2222.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit router mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface (ABC).
`(config-if)#isis circuit-type level-1`	Configure instance as level-1-only routing.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#isis circuit-type level-1`	Configure instance as level-1-only routing.
`(config-if)#exit`	Exit interface mode.
`(config)#mac vrf vrf_evpn_100`	Configure a new VRF named `vrf_evpn_100`.
`(config-vrf)#rd 2.2.2.1:1`	Assign the Route Distinguisher value.
`(config-vrf)#route-target both 100:1`	Configure route target to import and export the routes.
`(config-vrf)#exit`	Exit VRF mode.
`(config)#router bgp 1`	Define the routing process. The number 1 specifies the AS number of VTEP1.
`(config-router)#neighbor 1.1.1.1 remote-as 1`	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 1 is the neighbor's AS number.
`(config-router)# neighbor 1.1.1.1 update-source 2.2.2.2`	Define BGP neighbor: 2.2.2.2 is the peer interface.
`(config-router)#address-family l2vpn evpn`	Configure address-family L2VPN EVPN.

`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor in the EVPN address family.
`(config-router-af)#exit-address-family`	Exit address-family mode.
`(config-router)#exit`	Exit router mode.
`(config)#hardware-profile filter vxlan enable`	Enable hardware-profile filter for VXLAN.
`(config)#nvo vxlan enable`	Enable VXLAN globally on this VTEP.
`(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Assign a global IP to the VTEP.
`(config)#nvo vxlan id 100 ingress-replication`	Configure a VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf_evpn_100`.
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe1 2`	Configure access-port xe1 and map vlan 2
`(config-nvo-acc-if)#map vnid 100`	Map VNID 100 to access-port xe1.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan id 200 ingress-replication`	Configure second VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf_evpn_100`
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe2 3`	Configure access-port xe2 and map vlan 3
`(config-nvo-acc-if)#map vnid 200`	Map VNID 200 to access-port xe2.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.

Validation

CE1 and CE2 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	**IP Address**	**Mac Address**
VTEP1	CE-1	2	12.12.12.10	0000.0000.abab
VTEP2	CE-2	2	12.12.12.20	0000.0000.cdcd
VTEP1	CE-1	3	13.13.13.10	0000:0b60:25f2
VTEP2	CE-2	3	13.13.13.20	0000:0b60:25f3

Perform a tagged ping of VLAN 2 from CE1 to CE2 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2 and vice-versa.

VTEP Tunnel Status

```
VTEP-1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
```

```
1.1.1.1          2.2.2.2          Installed     00:05:53     00:05:53
Total number of entries are 1


VTEP-2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed     00:05:46     00:05:46
Total number of entries are 1
```

VTEP ARP Cache

```
VTEP-1#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID     Ip-Addr          Mac-Addr              Type                    Age-Out
Retries-Left
_____________________________________________________________________________
200      13.13.13.10    0000.0b60.25f2     Dynamic Local        246              2
200      13.13.13.20    0000.0b60.25f3     Dynamic Remote   ------
100      12.12.12.20    0000.0000.cdcd     Dynamic Remote   ------
100      12.12.12.10   0000.0000.abab     Dynamic Local        246              2
Total number of entries are 4

VTEP-2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID      Ip-Addr              Mac-Addr                Type                    Age-
Out       Retries-Left
_____________________________________________________________________________
200     13.13.13.10        0000.0b60.25f2       Dynamic Remote      -------
200     13.13.13.20       0000.0b60.25f3     Dynamic Local            257
2
100     12.12.12.10        0000.0000.abab      Dynamic Remote      -------
100     12.12.12.20       0000.0000.cdcd     Dynamic Local            257
2
Total number of entries are 4
```

VTEP MAC Tables

```
VTEP-1#show nvo vxlan mac-table
================================================================================
                                VXLAN MAC Entries
================================================================================
VNID   Interface   VlanId    Inner-VlanId    Mac-Addr        VTEP-Ip/ESI     Type
Status   AccessPortDesc
_____________________________________________________________________________
```

```
100      ----              ----           ----        0000.0000.cdcd      2.2.2.2
Dynamic Remote   -------    -------
100      xe1              2              ----        0000.0000.abab      1.1.1.1
Dynamic Local        -------    -------
200      xe2              3             ----        0000.0b60.25f2       1.1.1.1
Dynamic Local        -------    -------
200      ----             ----           ----        0000.0b60.25f3      2.2.2.2
Dynamic Remote   -------    -------
Total number of entries are : 4


VTEP-2#show nvo vxlan mac-table
================================================================================
                              VXLAN MAC Entries
================================================================================
VNID   Interface  VlanId    Inner-VlanId    Mac-Addr      VTEP-Ip/ESI     Type
Status     AccessPortDesc
________________________________________________________________________________


100      xe1            2          ----              0000.0000.cdcd     2.2.2.2
Dynamic Local      -------    -------
100      ----           ----       ----              0000.0000.abab     1.1.1.1
Dynamic Remote -------     -------
200      ----           ----       ----              0000.0b60.25f2      1.1.1.1
Dynamic Remote  -------     -------
200      xe2            3         ----              0000.0b60.25f3      2.2.2.2
Dynamic Local      -------     -------
Total number of entries are : 4
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI              Eth-Tag      Mac-Address           IP-Address     VNID     L3VNID
Nexthop         GW-Type
0                  100        0000:0000:abab    12.12.12.10    100      0
1.1.1.1             --
0                  200        0000:0b60:25f2     13.13.13.10    200      0
1.1.1.1             --

RD[2.2.2.2:1]
ESI         Eth-Tag     Mac-Address        IP-Address   VNID     L3VNID   Nexthop
GW-Type
0                100        0000:0000:cdcd     12.12.12.20    100          0
2.2.2.2             --
0                200        0000:0b60:25f3     13.13.13.20    200          0
2.2.2.2             --


VTEP-2#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI              Eth-Tag     Mac-Address        IP-Address          VNID      L3VNID
Nexthop         GW-Type
```

```
0                100         0000:0000:abab     12.12.12.10       100         0
1.1.1.1               --
0                200         0000:0b60:25f2     13.13.13.10       200         0
1.1.1.1               --

RD[2.2.2.2:1] VRF[vrf_evpn_100]:
ESI                 Eth-Tag     Mac-Address          IP-Address        VNID       L3VNID
Nexthop          GW-Type
0                  100         0000:0000:cdcd     12.12.12.20      100         0
2.2.2.2                --
0                  100         0000:0b60:25f2     13.13.13.10      100         0
2.2.2.2                --
```

LAG as Access Port with ECMP on the Network Side

This section contains basic VXLAN EVPN configuration with LAG as an access port and ECMP on the network side.

Topology

The procedures in this section use the topology in Figure 2-127.

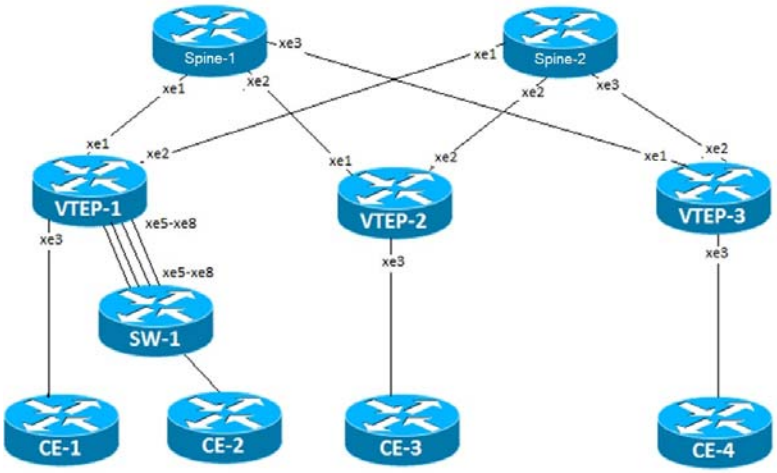


Figure 2-127: VXLAN EVPN with LAG and ECMP

SW-1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE vlan bridge
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure vlan 2 and associate with bridge 1
`(config-vlan)#vlan 3 bridge 1 state enable`	Configure vlan 3 and associate with bridge 1
`(config-vlan)#exit`	Exit from the vlan database
`(config)#in xe41`	Enter interface mode
`(config-if)#no shutdown`	Make interface admin up
`(config-if)#switchport`	Set the interface as Layer2 port

(config-if)#bridge-group 1	Associate the Interface with bridge-group.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode
(config-if)#switchport trunk allowed vlan add 2	Configure the VLANs that should be allowed through this interface
(config-if)#switchport trunk allowed vlan add 3	Configure the VLANs that should be allowed through this interface
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#exit	Exit interface mode.
(config)#in xe29	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe30	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe31	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe32	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config-if)#inter po1	Enter interface mode
(config-if)#bridge-group 1	Associate the Interface with bridge-group.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode
(config-if)#switchport trunk allowed vlan add 2	Configure the VLANs that should be allowed through this interface
(config-if)#switchport trunk allowed vlan add 3	Configure the VLANs that should be allowed through this interface
(config-if)#exit	Exit interface mode.

VTEP-1

#configure terminal	Enter configure mode
(config)#interface po1	Create interface po1
(config-if)#switchport	Configure the interface as switchport.
(config-if)#exit	Exit interface mode

(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe5	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe6	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe7	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe8	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.1.1.0/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 1.1.1.1/32 secondary	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net	Set a Network Entity Title for this instance, specifying the
49.0001.1111.1111.1111.00	area address and the system ID.

(config-router)#exit	Exit router mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#bgp router-id 1.1.1.1	Configure router-id for this BGP process.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 65535 is the neighbor's AS number.
(config-router)# neighbor 2.2.2.2 update-source 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)# neighbor 3.3.3.3 update-source 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#hardware-profile filter vxlan enable	Enable hardware-profile filter for VXLAN.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 1.1.1.1	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.

`(config)#nvo vxlan access-if port-vlan xe3 2`	Configure access-port xe3 and map vlan 2
`(config-nvo-acc-if)#map vnid 100001`	Map VNID 100001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan access-if port-vlan po1 2`	Configure access-port po1 and map vlan 2
`(config-nvo-acc-if)#map vnid 100001`	Map VNID 100001 to access-port po1.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan id 200001 ingress-replication`	Configure second VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf_evpn_100.`
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe3 3`	Configure access-port xe3 and map vlan 3
`(config-nvo-acc-if)#map vnid 200001`	Map VNID 200001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan access-if port-vlan po1 3`	Configure access-port po1 and map vlan 3
`(config-nvo-acc-if)#map vnid 200001`	Map VNID 200001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.

Spine-1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 12.12.12.12/32 secondary`	Set an IP address on the interface.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/31`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/31`	Configure IP address on the interface xe2.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe3`	Enter intereface mode.
`(config-if)#ip address 30.1.1.1/31`	Configure IP address on the interface xe3.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance (ABC).
`(config-router)#is-type level-1`	Configure instance as level-1-only routing.

(config-router)#net 49.0001.4444.4444.4444.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

Spine-2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 13.13.13.13/32 secondary	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.1.1.3/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.3/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 30.1.1.3/31	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.

(config-router)#net 49.0001.5555.5555.5555.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP-2

#configure terminal	Enter configure mode
(config)#interface po1	Enter interface mode
(config-if)#switchport	Configure the interface as switchport
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 20.1.1.0/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.2/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation

(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.2222.2222.2222.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 update-source 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 3.3.3.3 update-source 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#hardware-profile filter vxlan enable	Enable hardware-profile filter for VXLAN.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 2.2.2.2	Assign a global IP to the VTEP.

`(config)#nvo vxlan id 100001 ingress-replication`	Configure a VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf_evpn_100`.
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe3 2`	Configure access-port xe3 and map vlan 2
`(config-nvo-acc-if)#map vnid 100001`	Map VNID 100001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan id 200001 ingress-replication`	Configure second VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf_evpn_100.`
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe3 3`	Configure access-port xe3 and map vlan 3
`(config-nvo-acc-if)#map vnid 200001`	Map VNID 200001 to access-port xe3.
`(config-nvo-acc-if)#exit-adress-family`	Exit NVO access-if mode.

VTEP-3

`#configure terminal`	Enter configure mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 30.1.1.0/31`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 30.1.1.2/31`	Configure IP address on the interface xe2.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Configure IP address on the loopback interface.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance (ABC).
`(config-router)#is-type level-1`	Configure instance as level-1-only routing.
`(config-router)#net 49.0001.3333.3333.3333.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit router mode.

(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 update-source 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 2.2.2.2 update-source 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#hardware-profile filter vxlan enable	Enable hardware-profile filter for VXLAN.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 3.3.3.3	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.

`(config-nvo-acc-if)#exit-address-family`	Exit NVO access-if mode.
`(config)#nvo vxlan id 200001 ingress-replication`	Configure second VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf_evpn_100`
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe3 3`	Configure access-port xe3 and map vlan 3
`(config-nvo-acc-if)#map vnid 200001`	Map VNID 200001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.

Validation

CE1, CE2, CE3, and CE4 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	IP Address	MAC Address
VTEP1	CE-1	2	12.12.12.10	0000.0000.aaaa
VTEP1	CE-2	2	12.12.12.20	0000.0000.bbbb
VTEP2	CE-3	2	12.12.12.30	0000.0000.cccc
VTEP3	CE-4	2	12.12.12.40	0000.0000.dddd
VTEP1	CE-1	3	14.14.14.10	0000.058e.2181
VTEP1	CE-2	3	14.14.14.20	0000.058e.2182
VTEP2	CE-3	3	14.14.14.30	0000.058e.2183
VTEP3	CE-4	3	14.14.14.40	0000.058e.2184

Perform a tagged ping of VLAN 2 from CE1 to CE2,CE3 and CE4 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2, CE3 and CE4 and vice-versa.

VTEP Tunnel Status

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          3.3.3.3          Installed     01:25:20     01:25:20
1.1.1.1          2.2.2.2          Installed     01:35:19     01:35:19
Total number of entries are 2

VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed     01:35:42     01:35:42
2.2.2.2          3.3.3.3          Installed     01:25:43     01:25:43
```

```
Total number of entries are 2

VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
3.3.3.3          2.2.2.2          Installed     01:25:35     01:25:35
3.3.3.3          1.1.1.1          Installed     01:25:35     01:25:35
Total number of entries are 2
```

VTEP ARP Tables

```
VTEP-1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID     Ip-Addr           Mac-Addr            Type         Age-Out    Retries-Left
_____________________________________________________________________________
200      13.13.13.10    0000.0b60.25f2     Dynamic Local        246              2
200      13.13.13.20    0000.0b60.25f3     Dynamic Remote   ------
100      12.12.12.20    0000.0000.cdcd     Dynamic Remote   ------
100      12.12.12.10    0000.0000.abab     Dynamic Local        246              2
Total number of entries are 4


VTEP-2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID      Ip-Addr          Mac-Addr               Type        Age-Out    Retries-Left
_____________________________________________________________________________
200     13.13.13.10       0000.0b60.25f2      Dynamic Remote  -------
200      13.13.13.20      0000.0b60.25f3      Dynamic Local      257           2
100     12.12.12.10       0000.0000.abab      Dynamic Remote   -------
100      12.12.12.20      0000.0000.cdcd      Dynamic Local      257            2
Total number of entries are 4


VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
100001   12.12.12.30      0000.0000.cccc Dynamic Remote ----
100001   12.12.12.10      0000.0000.aaaa Dynamic Remote ----
100001   12.12.12.20      0000.0000.bbbb Dynamic Remote ----
100001   12.12.12.40      0000.0000.dddd Dynamic Local  ----
200001   14.14.14.20      0000.058e.2182 Dynamic Remote ----
200001   14.14.14.10      0000.058e.2181 Dynamic Remote ----
200001   14.14.14.40      0000.058e.2184 Dynamic Local  ----
200001   14.14.14.30      0000.058e.2183 Dynamic Remote ----
```

```
Total number of entries are 8
VTEP3#
```

VTEP MAC Tables

```
VTEP1#show nvo vxlan mac-table

================================================================================
================================================================================
                              VXLAN MAC Entries
================================================================================
================================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                 Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         xe1/1      1000   2000         0000.339a.9abb 33.33.33.0
       Dynamic Local        -------             -------
1         ----       ----   ----         0000.339a.9397 34.34.34.0
       Dynamic Remote       -------             -------

Total number of entries are : 2

VTEP2#show nvo vxlan mac-table
================================================================================
================================================================================
                              VXLAN MAC Entries
================================================================================
================================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                 Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         ----       ----   ----         0000.339a.9abb 33.33.33.0
       Dynamic Remote       -------             -------
1         xe1/1      1000   2000         0000.339a.9397 34.34.34.0
       Dynamic Local        -------             -------

Total number of entries are : 2
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI              Eth-Tag      Mac-Address           IP-Address     VNID     L3VNID
Nexthop         GW-Type
0                   100        0000:0000:abab    12.12.12.10    100      0
1.1.1.1              --
```

```
0                  200        0000:0b60:25f2     13.13.13.10    200      0
1.1.1.1             --

RD[2.2.2.2:1]
ESI          Eth-Tag     Mac-Address         IP-Address    VNID     L3VNID   Nexthop
GW-Type
0                 100        0000:0000:cdcd     12.12.12.20    100           0
2.2.2.2              --
0                  200        0000:0b60:25f3     13.13.13.20    200           0
2.2.2.2              --


VTEP-2#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI              Eth-Tag     Mac-Address         IP-Address           VNID      L3VNID
Nexthop          GW-Type
0                 100        0000:0000:abab     12.12.12.10       100         0
1.1.1.1              --
0                 200        0000:0b60:25f2     13.13.13.10       200         0
1.1.1.1              --

RD[2.2.2.2:1] VRF[vrf_evpn_100]:
ESI                Eth-Tag     Mac-Address         IP-Address       VNID      L3VNID
Nexthop          GW-Type
0                   100        0000:0000:cdcd     12.12.12.20     100         0
2.2.2.2                   --
0                   100        0000:0b60:25f2     13.13.13.10     100         0
2.2.2.2                   --


VTEP-3#show bgp l2vpn evpn mac-ip

RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI                        Eth-Tag    Mac-Address    IP-Address
VNID      L3VNID    Nexthop          GW-Type
0                           100001     0000:0000:dddd --
100001    0         3.3.3.3          --
0                          100001     0000:0000:dddd 12.12.12.40
100001    0         3.3.3.3          --
0                           200001     0000:058e:2184 --
200001    0         3.3.3.3          --
0                          200001     0000:058e:2184 14.14.14.40
200001    0         3.3.3.3          --

RD[1.1.1.1:1]
ESI                        Eth-Tag    Mac-Address    IP-Address
VNID      L3VNID    Nexthop          GW-Type
0                           100001     0000:0000:aaaa --
100001    0         1.1.1.1          --
0                          100001     0000:0000:aaaa 12.12.12.10
100001    0         1.1.1.1          --
0                           100001     0000:0000:bbbb --
100001    0         1.1.1.1          --
0                          100001     0000:0000:bbbb 12.12.12.20
100001    0         1.1.1.1          --
```

```
0                       100001     0000:0000:cccc --
100001    0         2.2.2.2         --
0                       100001     0000:0000:cccc 12.12.12.30
100001    0         2.2.2.2         --
0                       200001     0000:058e:2181 --
200001    0         1.1.1.1         --
0                       200001     0000:058e:2181 14.14.14.10
200001    0         1.1.1.1         --
0                       200001     0000:058e:2182 --
200001    0         1.1.1.1         --
0                       200001     0000:058e:2182 14.14.14.20
200001    0         1.1.1.1         --
0                       200001     0000:058e:2183 --
200001    0         2.2.2.2         --
0                       200001     0000:058e:2183 14.14.14.30
200001    0         2.2.2.2         --
```

CHAPTER 3 VxLAN Multi-Homing Configuration

This chapter contains the configurations for VxLAN Multi-homing feature.

Overview

VxLAN EVPN Multi-homing features enables to connect a CE/Host node to two VTEPs with all-active redundancy mode. A redundant VTEP device can provide network service to the customer site as soon as a failure is detected. The failure can be link or node failure. If one VTEP goes down, other will forward the entire traffic.

Below are Multi-homing concepts:

- Ethernet Segment: Set of links which connect host/CE to two active-active multi-homed VTEP (only two VTEPs are supported) which appears as LACP link for host.
- Ethernet Segment Identifier: Ethernet Segment Identifier (ESI) which is a 10 octet-value, which can be configured in two ways, system MAC is configured as esi in case of Dynamic LAG and 10-octet ESI format configuration is used on physical interface ES.
- Ethernet Segment Route (ES route): When a multi-homed CE is configured as an VXLAN access-port, Ethernet segment route is sent. The main purpose of this route is to discover other VTEPs which share the ES and to perform DF election.
- Ethernet A-D route per ESI: This route is used for Fast Convergence and Split Horizon.
- Ethernet A-D route per EVI: This route is used for load sharing between DF and NON-DF by the remote VTEPs

Topology

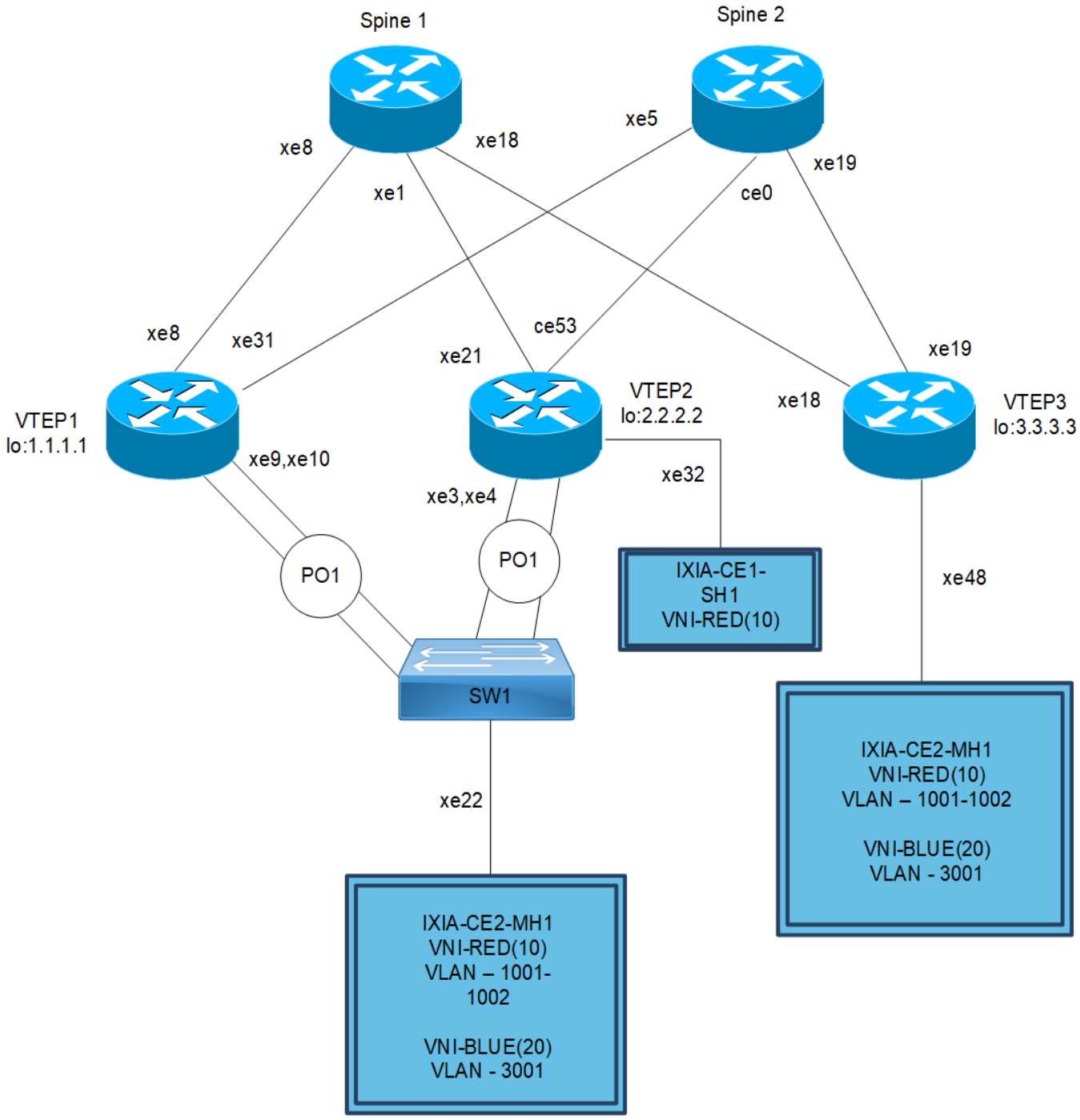


Figure 3-128: VxLAN-Multihoming

ESI can be configured in below two ways

Ethernet Segment through Dynamic LAG interface

`#configure terminal`	Enter Configure mode.
`(config)#interface po1`	Enter Interface mode for po1
`(config-if)#switchport`	Make it L2 interface
`(config-if)#evpn multi-homed system-mac 8899.4400.6745`	Configure system mac as ESI value for LAG (po1) interface
`(config-if)#exit`	Exit Interface mode.

OR

Ethernet Segment through Physical or Static LAG interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe41`	Enter Interface mode for xe41
`(config-if)#switchport`	Make it L2 interface
`(config-if)# evpn multi-homed esi 00:01:02:03:04:05:06:07:08`	Configure 9-octet ESI value for xe41 interface (in static config, out of 10-octet ESI value, first octet is reserved)
`(config-if)#exit`	Exit Interface mode.

VTEP1

(Multi-homed group1) – Part of both Multi-homed with po1 (MH1)

Hardware Profile and Generic Configuration

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter vxlan enable`	Enable hardware-profile filter for VXLAN.
`(config)#hardware-profile filter vxlan-mh enable`	Enable hardware-profile filter for VXLAN multi-homing.
`(config)#hardware-profile filter egress-ipv4 enable`	Enable hardware-profile filter for egress IPv4.
`(config)#evpn vxlan multihoming enable`	Enable Multihoming, save configs and reboot the board for multihoming to be effective
`(config)#hardware-profile statistics ac-lif enable`	Enable ac-lif for VxLAN access-if port counters
`(config)#qos enable`	Enabling QoS

Interface and Loopback Configuration

`(config)#interface po1`	Enter Interface mode for po1 (MH1)
`(config-if)#switchport`	Make it L2 interface
`(config-if)# evpn multi-homed system-mac 0000.0000.1111`	Configure system MAC as ESI value for LAG (po1) interface
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

(config)#interface xe9	Enter Interface mode for xe9
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe10	Enter Interface mode for xe10
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface lo	Enter Interface mode for lo
(config-if)#ip address 1.1.1.1/32 secondary	Configure loopback ip address as 1.1.1.1 for VTEP1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe8	Enter Interface mode for xe8
(config-if)#ip address 10.10.10.1/24	Configure IP address as 10.10.10.1 on network side of Spine1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe31	Enter Interface mode for xe31
(config-if)#ip address 20.20.20.1/24	Configure IP address as 20.20.20.1 on network side of Spine2
(config-if)#exit	Exit Interface mode and return to Configure mode.

OSPF Configuration

(config)#router ospf 100	Enter into router OSPF mode
(config-router)#ospf router-id 1.1.1.1	Configure router-id as 1.1.1.1 (lo ip address)
(config-router)#network 1.1.1.1/32 area 0.0.0.0	Add 1.1.1.1 (lo IP address) network into area 0
(config-router)#network 10.10.10.0/24 area 0.0.0.0	Add 10.10.10.0 (Spine1) network into area 0
(config-router)#network 20.20.20.0/24 area 0.0.0.0	Add 20.20.20.0 (Spine2) network into area 0
(config-router)#bfd all-interfaces	Enabling BFD on all OSPF interface for fast convergence
(config-if)#exit	Exit Interface mode and return to Configure mode.

BGP Configuration

(config)#router bgp 500	Enter into Router BGP mode
(config-router)#bgp router-id 1.1.1.1	Configure router-id as 1.1.1.1 (lo IP address)
(config-router)#network 1.1.1.1/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 2.2.2.2 remote-as 500	Specify a VTEP2 loopback IP address and remote-as defined
(config-router)#neighbor 2.2.2.2 update-source lo	Configure update as loopback for VTEP2
(config-router)#neighbor 2.2.2.2 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP2
(config-router)#neighbor 3.3.3.3 remote-as 500	Specify a VTEP3 loopback IP address and remote-as defined
(config-router)#neighbor 3.3.3.3 update-source lo	Configure update as loopback for VTEP3

(config-router)#neighbor 3.3.3.3 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP3
(config-router)#address-family l2vpn evpn	Enter into L2VPN EVPN address family mode
(config-router-af)#neighbor 2.2.2.2 activate	Activate 2.2.2.2 (VTEP2) into L2VPN evpn address family mode
(config-router-af)#neighbor 3.3.3.3 activate	Activate 3.3.3.3 (VTEP3) into L2VPN evpn address family mode
(config-router-af)#exit-address-family	Exit from L2VPN address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode

VRF Configuration

(config)#mac vrf VRF1	Create mac routing/forwarding instance with VRF1 name and enter into VRF mode
(config-vrf)#rd 1.1.1.1:11	Assign RD value
(config-vrf)#route-target both 9.9.9.9:100	Assign route-target value for same for import and export. Should be same on all node for VRF1
(config-vrf)#exit	Exit from VRF mode
(config)#mac vrf VRF2	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
(config-vrf)#rd 1.1.1.1:21	Assign RD value
(config-vrf)#route-target both 90.90.90.90:100	Assign route-target value for same for import and export
(config-vrf)#exit	Exit from VRF mode

VxLAN Configuration

(config)#nvo vxlan enable	Enable VxLAN
(config)#evpn esi hold-time 60	Configure ESI hold time to allow tunnel to come up at the time of VxLAN initialization before making the ESI up
(config)#nvo vxlan vtep-ip-global 1.1.1.1	Configure Source VTEP-IP-global configuration
(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1	Assign VRF for EVPN-BGP to carry EVPN route
(config-nvo)#vni-name VNI-RED	Configure VNI-name as VNI-RED
(config-nvo)#exit	Exit from VxLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2	Assign VRF for EVPN-BGP to carry EVPN route
(config-nvo)#vni-name VNI-BLUE	Configure VNI-name as VNI-BLUE
(config-nvo)#exit	Exit from VxLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan po1 1001	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port

(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan po1 1002	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan po1 3001	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-BLUE	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

VTEP2

(Multi-homed group1) – Part of both Multi-homed with po1 (MH1). And it has xe32 as single home access-if port (SH2)

Hardware Profile and Generic Configuration

#configure terminal	Enter Configure mode.
(config)#hardware-profile filter vxlan enable	Enable hardware-profile filter for VxLAN.
(config)#hardware-profile filter vxlan-mh enable	Enable hardware-profile filter for VxLAN multi-homing.
(config)#hardware-profile filter egress-ipv4 enable	Enable hardware-profile filter for egress IPv4.
(config)#evpn vxlan multihoming enable	Enable Multihoming, save configs and reboot the board for multihoming to be effective
(config)#hardware-profile statistics ac-lif enable	Enable ac-lif for VxLAN access-if port counters
(config)#qos enable	Enabling QoS

Interface and Loopback Configuration

(config)#interface po1	Enter Interface mode for po1 (MH1)
(config-if)#switchport	Make it L2 interface
(config-if)# evpn multi-homed system-mac 0000.0000.1111	Configure system MAC as ESI value for LAG (po1) interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe3	Enter Interface mode for xe3
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe4	Enter Interface mode for xe4
(config-if)#channel-group 1 mode active	Make it member port of po1

(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe32	Enter Interface mode for xe32 (SH2)
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface lo	Enter Interface mode for lo
(config-if)#ip address 2.2.2.2/32 secondary	Configure loopback IP address as 2.2.2.2 for VTEP2
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe21	Enter Interface mode for xe21
(config-if)#ip address 30.30.30.1/24	Configure IP address as 30.30.30.1 on network side of Spine1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface ce53	Enter Interface mode for ce53
(config-if)#ip address 40.40.40.1/24	Configure IP address as 40.40.40.1 on network side of Spine2
(config-if)#exit	Exit Interface mode and return to Configure mode.

OSPF Configuration

(config)#router ospf 100	Enter into router OSPF mode
(config-router)#ospf router-id 2.2.2.2	Configure router-id as 2.2.2.2 (lo IP address)
(config-router)#network 2.2.2.2/32 area 0.0.0.0	Add 2.2.2.2 (lo IP address) network into area 0
(config-router)#network 30.30.30.0/24 area 0.0.0.0	Add 30.30.30.0 (Spine1) network into area 0
(config-router)#network 40.40.40.0/24 area 0.0.0.0	Add 40.40.40.0 (Spine2) network into area 0
(config-router)#bfd all-interfaces	Enabling BFD on all OSPF interface for fast convergence
(config-if)#exit	Exit Interface mode and return to Configure mode.

BGP Configuration

(config)#router bgp 500	Enter into Router BGP mode
(config-router)#bgp router-id 2.2.2.2	Configure router-id as 2.2.2.2 (lo IP address)
(config-router)#network 2.2.2.2/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 1.1.1.1 remote-as 500	Specify a VTEP1 loopback IP address and remote-as defined
(config-router)#neighbor 1.1.1.1 update-source lo	Configure update as loopback for VTEP1
(config-router)#neighbor 1.1.1.1 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP1
(config-router)#neighbor 3.3.3.3 remote-as 500	Specify a VTEP3 loopback IP address and remote-as defined
(config-router)#neighbor 3.3.3.3 update-source lo	Configure update as loopback for VTEP3
(config-router)#neighbor 3.3.3.3 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP3
(config-router)#address-family l2vpn evpn	Enter into L2VPN EVPN address family mode

`(config-router-af)#neighbor 1.1.1.1 activate`	Activate 1.1.1.1(VTEP1) into L2VPN evpn address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate 3.3.3.3(VTEP3) into L2VPN evpn address family mode
`(config-router-af)#exit-address-family`	Exit from L2VPN address family mode
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode

VRF Configuration

`(config)# mac vrf VRF1`	Create mac routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 2.2.2.2:11`	Assign RD value
`(config-vrf)#route-target both 9.9.9.9:100`	Assign route-target value for same for import and export. Should be same on all node for VRF1
`(config-vrf)#exit`	Exit from VRF mode
`(config)#mac vrf VRF2`	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 2.2.2.2:21`	Assign RD value
`(config-vrf)#route-target both 90.90.90.90:100`	Assign route-target value for same for import and export
`(config-vrf)#exit`	Exit from VRF mode

VxLAN Configuration

`(config)#nvo vxlan enable`	Enable VxLAN
`(config)#evpn esi hold-time 60`	Configure ESI hold time to allow tunnel to come up at the time of VxLAN initialization before making the ESI up
`(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Configure Source VTEP-IP-global configuration
`(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-RED`	Configure VNI-name as VNI-RED
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-BLUE`	Configure VNI-name as VNI-BLUE
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan access-if port-vlan po1 1001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode

(config)#nvo vxlan access-if port-vlan po1 1002	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan po1 3001	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-BLUE	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port xe32	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

VTEP3

It has xe48 as Single home access-if port (SH2)

Hardware Profile and Generic Configuration

#configure terminal	Enter Configure mode.
(config)#hardware-profile filter vxlan enable	Enable hardware-profile filter for VxLAN.
(config)#hardware-profile filter vxlan-mh enable	Enable hardware-profile filter for VxLAN multi-homing.
(config)#hardware-profile filter egress-ipv4 enable	Enable hardware-profile filter for egress IPv4.
(config)#evpn vxlan multihoming enable	Enable Multihoming, save configs and reboot the board for multihoming to be effective
(config)#hardware-profile statistics ac-lif enable	Enable ac-lif for VxLAN access-if port counters
(config)#qos enable	Enabling QoS

Interface and loopback configuration

(config)#interface xe48	Enter Interface mode for xe48 (SH3)
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface lo	Enter Interface mode for lo
(config-if)#ip address 3.3.3.3/32 secondary	Configure loopback IP address as 3.3.3.3 for VTEP3
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe18	Enter Interface mode for xe18
(config-if)#ip address 50.50.50.1/24	Configure IP address as 50.50.50.1 on network side of Spine1

(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe19	Enter Interface mode for xe19
(config-if)#ip address 60.60.60.1/24	Configure IP address as 60.60.60.1 on network side of Spine2
(config-if)#exit	Exit Interface mode and return to Configure mode.

OSPF Configuration

(config)#router ospf 100	Enter into router OSPF mode
(config-router)#ospf router-id 2.2.2.2	Configure router-ID as 2.2.2.2 (lo IP address)
(config-router)#network 2.2.2.2/32 area 0.0.0.0	Add 2.2.2.2 (lo IP address) network into area 0
(config-router)#network 50.50.50.0/24 area 0.0.0.0	Add 50.50.50.0 (Spine1) network into area 0
(config-router)#network 60.60.60.0/24 area 0.0.0.0	Add 60.60.60.0 (Spine2) network into area 0
(config-router)#bfd all-interfaces	Enabling BFD on all OSPF interface for fast convergence
(config-if)#exit	Exit Interface mode and return to Configure mode.

BGP Configuration

(config)#router bgp 500	Enter into Router BGP mode
(config-router)#bgp router-id 3.3.3.3	Configure router-ID as 3.3.3.3 (lo ip address)
(config-router)#network 3.3.3.3/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 1.1.1.1 remote-as 500	Specify a VTEP1 loopback IP address and remote-as defined
(config-router)#neighbor 1.1.1.1 update-source lo	Configure update as loopback for VTEP1
(config-router)#neighbor 1.1.1.1 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP1
(config-router)#neighbor 2.2.2.2 remote-as 500	Specify a VTEP2 loopback IP address and remote-as defined
(config-router)#neighbor 2.2.2.2 update-source lo	Configure update as loopback for VTEP2
(config-router)#neighbor 2.2.2.2 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP3
(config-router)#address-family l2vpn evpn	Enter into L2VPN EVPN address family mode
(config-router-af)#neighbor 1.1.1.1 activate	Activate 1.1.1.1 (VTEP1) into L2VPN evpn address family mode
(config-router-af)#neighbor 2.2.2.2 activate	Activate 2.2.2.2 (VTEP2) into L2VPN evpn address family mode
(config-router-af)#exit-address-family	Exit from L2VPN address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode

VRF Configuration

(config)# mac vrf VRF1	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
(config-vrf)#rd 3.3.3.3:11	Assign RD value
(config-vrf)#route-target both 9.9.9.9:100	Assign route-target value for same for import and export. Should be same on all node for VRF1
(config-vrf)#exit	Exit from VRF mode
(config)#mac vrf VRF2	Create MAC routing/forwarding instance with VRF2 name and enter into VRF mode
(config-vrf)#rd 3.3.3.3:21	Assign RD value
(config-vrf)#route-target both 90.90.90.90:100	Assign route-target value for same for import and export
(config-vrf)#exit	Exit from VRF

VxLAN Configuration

(config)#nvo vxlan enable	Enable VxLAN
(config)#nvo vxlan vtep-ip-global 3.3.3.3	Configure Source VTEP-IP-global configuration
(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1	Assign VRF for EVPN-BGP to carry EVPN route
(config-nvo)#vni-name VNI-RED	Configure VNI-name as VNI-RED
(config-nvo)#exit	Exit from VxLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2	Assign VRF for EVPN-BGP to carry EVPN route
(config-nvo)#vni-name VNI-BLUE	Configure VNI-name as VNI-BLUE
(config-nvo)#exit	Exit from VxLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan xe48 1001	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan xe48 1002	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan xe48 3001	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-BLUE	Map VxLAN Identified to access-port for VxLAN

`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#exit`	Exit from configuration mode

Switch (CE2)

Multihomed to 2-VTEPs (VTEP1 and VTEP2)

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE VLAN bridge
`(config)#vlan 1001-1002 bridge 1 state enable`	Configure VLANs from 1001-1002 and associate with bridge 1
`(config)#vlan 3001 bridge 1 state enable`	Configure VLANs from 3001 and associate with bridge 1
`(config)#interface xe22`	Enter Interface mode for xe22
`(config-if)#switchport`	Make xe22 as L2 port by configuring switchport
`(config-if)#bridge-group 1`	Associate xe22 to bridge 1
`(config-if)#switchport mode hybrid`	Configure xe22 as hybrid port
`(config-if)#switchport hybrid allowed vlan add 1001-1002,3001 egress-tagged enable`	Allow 1001-1002 and 3001 configured VLANs on xe22
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface po1`	Enter Interface mode for po1
`(config-if)#switchport`	Make po1 as L2 port by configuring switchport
`(config-if)#bridge-group 1`	Associate po1 to bridge 1
`(config-if)#switchport mode hybrid`	Configure po1 as hybrid port
`(config-if)#switchport hybrid allowed vlan add 1001-1002,3001 egress-tagged enable`	Allow 1001-1002 and 3001 configured VLANs on po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe3`	Enter Interface mode for xe3
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#interface xe4`	Enter Interface mode for xe4
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#exit`	Exit from configuration mode
`(config)#interface xe9`	Enter Interface mode for xe9
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#interface xe10`	Enter Interface mode for xe10
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#exit`	Exit from configuration mode

Spine 1

Spine node where all VTEPs are connected

Generic Configuration

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling QoS

Interface and Loopback Configuration

`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure loopback IP address as 11.11.11.11 for Spine1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe8`	Enter Interface mode for xe8
`(config-if)#ip address 10.10.10.2/24`	Configure IP address as 10.10.10.2 on network side of VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1
`(config-if)#ip address 30.30.30.2/24`	Configure IP address as 30.30.30.2 on network side of VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe18`	Enter Interface mode for xe18
`(config-if)#ip address 50.50.50.2/24`	Configure IP address as 50.50.50.2 on network side of VTEP3
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 11.11.11.11`	Configure router-ID as 11.11.11.11 (lo IP address)
`(config-router)#network 11.11.11.11/32 area 0.0.0.0`	Add 11.11.11.11 (lo IP address) network into area 0
`(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add 10.10.10.0 (VTEP1) network into area 0
`(config-router)#network 30.30.30.0/24 area 0.0.0.0`	Add 30.30.30.0 (VTEP2) network into area 0
`(config-router)#network 50.50.50.0/24 area 0.0.0.0`	Add 50.50.50.0 (VTEP3) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Spine 2

Spine node where all VTEPs are connected

Generic configuration

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling QoS

Interface and loopback configuration

`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure loopback IP address as 22.22.22.22 for Spine2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe5`	Enter Interface mode for xe5
`(config-if)#ip address 20.20.20.2/24`	Configure IP address as 20.20.20.2 on network side of VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface ce0`	Enter Interface mode for ce0
`(config-if)#ip address 40.40.40.2/24`	Configure IP address as 40.40.40.2 on network side of VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe19`	Enter Interface mode for xe19
`(config-if)#ip address 60.60.60.2/24`	Configure IP address as 60.60.60.2 on network side of VTEP3
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 22.22.22.22`	Configure router-id as 11.11.11.11 (lo IP address)
`(config-router)#network 22.22.22.22/32 area 0.0.0.0`	Add 22.22.22.22 (lo IP address) network into area 0
`(config-router)#network 20.20.20.0/24 area 0.0.0.0`	Add 20.20.20.0 (VTEP1) network into area 0
`(config-router)#network 40.40.40.0/24 area 0.0.0.0`	Add 40.40.40.0 (VTEP2) network into area 0
`(config-router)#network 60.60.60.0/24 area 0.0.0.0`	Add 60.60.60.0 (VTEP3) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Validation

VTEP1

```
VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
```

```
        (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                            VLAN DF-Status Src-Addr        Dst-Addr
-------------------------------------------------------------------------------------------------------------------
10       VNI-RED      L2       NW   ----      ----                           ---- ----      1.1.1.1         3.3.3.3
10       VNI-RED      L2       NW   ----      ----                           ---- ----      1.1.1.1         2.2.2.2
10       VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1001 NON-DF    ----            ----
10       VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1002 DF        ----            ----
20       VNI-BLUE     L2       NW   ----      ----                           ---- ----      1.1.1.1         3.3.3.3
20       VNI-BLUE     L2       NW   ----      ----                           ---- ----      1.1.1.1         2.2.2.2
20       VNI-BLUE     --       AC   po1       00:00:00:00:00:11:11:00:00:00 3001 NON-DF    ----            ----

Total number of entries are 7
```

```
VTEP1#show nvo vxlan access-if brief

                 Inner                      Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid       status  status
-----------------------------------------------------------
po1        1002  ---   500001   10         up      up
po1        1001  ---   500000   10         up      up
po1        3001  ---   500002   20         up      up

Total number of entries are 3
```

```
VTEP1#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 500
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd     AD  MACIP  MCAST    ESI
PREFIX-ROUTE
2.2.2.2                  4   500  161       163       5     0      0  01:05:15             6      3      0      2      1      0
3.3.3.3                  4   500  157       161       5     0      0  01:05:07             2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
```

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
1.1.1.1          3.3.3.3          Installed        00:31:11       00:31:11
1.1.1.1          2.2.2.2          Installed        01:05:25       00:31:11

Total number of entries are 2
```

```
VTEP1#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
ESI                           PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  1.1.1.1         1.1.1.1         VXLAN
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN

RD[2.2.2.2:1]
ESI                           PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN
```

```
VTEP1#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

RD[1.1.1.1:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN

RD[2.2.2.2:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN
VTEP1#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   20          20             1.1.1.1         VXLAN

RD[2.2.2.2:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN

RD[2.2.2.2:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN

VTEP1#show bgp l2vpn evpn
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf      Weight     Path  Peer         Encap
```

```
RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1             0        100          32768    i  ----------      VXLAN
*>   [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                     1.1.1.1             0        100          32768    i  ----------      VXLAN
* i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN

RD[1.1.1.1:11] VRF[VRF1]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>                   1.1.1.1             0        100          32768    i  ----------      VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>   [3]:[10]:[32,1.1.1.1]
                     1.1.1.1             0        100          32768    i  ----------      VXLAN
* i  [3]:[10]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
* i  [3]:[10]:[32,3.3.3.3]
                     3.3.3.3             0        100          0        i  3.3.3.3         VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>                   1.1.1.1             0        100          32768    i  ----------      VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>   [3]:[20]:[32,1.1.1.1]
                     1.1.1.1             0        100          32768    i  ----------      VXLAN
* i  [3]:[20]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
* i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0        100          0        i  3.3.3.3         VXLAN

RD[2.2.2.2:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN

RD[2.2.2.2:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>i  [3]:[10]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN

RD[2.2.2.2:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN
*>i  [3]:[20]:[32,2.2.2.2]
                     2.2.2.2             0        100          0        i  2.2.2.2         VXLAN

RD[3.3.3.3:11]
*>i  [3]:[10]:[32,3.3.3.3]
                     3.3.3.3             0        100          0        i  3.3.3.3         VXLAN

RD[3.3.3.3:21]
*>i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0        100          0        i  3.3.3.3         VXLAN
```

```
Total number of prefixes 21
```

VTEP2

```
VTEP2#show nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status Src-Addr         Dst-Addr
-------------------------------------------------------------------------------------------------------------------
10       VNI-RED      L2       NW   ----      ----                         ---- ----      2.2.2.2         1.1.1.1
10       VNI-RED      L2       NW   ----      ----                         ---- ----      2.2.2.2         3.3.3.3
10       VNI-RED      --       AC   xe32      --- Single Homed Port ---     ---- ----      ----            ----
10       VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1001 DF        ----            ----
10       VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1002 NON-DF    ----            ----
20       VNI-BLUE     L2       NW   ----      ----                         ---- ----      2.2.2.2         1.1.1.1
20       VNI-BLUE     L2       NW   ----      ----                         ---- ----      2.2.2.2         3.3.3.3
20       VNI-BLUE     --       AC   po1       00:00:00:00:00:11:11:00:00:00 3001 DF        ----            ----

Total number of entries are 8
```

```
VTEP2#show nvo vxlan access-if
% Incomplete command.

VTEP2#show nvo vxlan access-if brief

                 Inner                      Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid       status  status
-----------------------------------------------------------
xe32       ---   ---   500004   10         up      up
po1        1002  ---   500001   10         up      up
po1        1001  ---   500000   10         up      up
po1        3001  ---   500002   20         up      up

Total number of entries are 4
```

```
VTEP2#show bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 500
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd     AD  MACIP  MCAST    ESI
PREFIX-ROUTE
1.1.1.1                 4   500  172       171      4      0      0  01:09:28            6      3      0      2      1      0
3.3.3.3                 4   500  165       173      4      0      0  01:09:29            2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
```

```
VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
=============================================================================
2.2.2.2          1.1.1.1          Installed        01:09:38       00:35:24
2.2.2.2          3.3.3.3          Installed        01:09:39       01:09:39
```

```
Total number of entries are 2

VTEP2#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1]
ESI                           PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  1.1.1.1         1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
ESI                           PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  1.1.1.1         1.1.1.1         VXLAN
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN
VTEP2#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

VTEP2#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11]
ESI                              Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21]
ESI                              Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
ESI                              Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
ESI                              Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN

VTEP2# show bgp l2vpn evpn
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[1.1.1.1:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[1.1.1.1:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [3]:[10]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[1.1.1.1:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [3]:[20]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     2.2.2.2             0         100          32768    i  ----------      VXLAN
* i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>   [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                     2.2.2.2             0         100          32768    i  ----------      VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     2.2.2.2             0         100          32768    i  ----------      VXLAN
* i                   1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
* i  [3]:[10]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>   [3]:[10]:[32,2.2.2.2]
                     2.2.2.2             0         100          32768    i  ----------      VXLAN
* i  [3]:[10]:[32,3.3.3.3]
                     3.3.3.3             0         100          0        i  3.3.3.3         VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                     2.2.2.2             0         100          32768    i  ----------      VXLAN
* i                   1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
* i  [3]:[20]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>   [3]:[20]:[32,2.2.2.2]
```

```
                     2.2.2.2             0         100          32768    i  ----------      VXLAN
* i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0         100          0        i  3.3.3.3         VXLAN

RD[3.3.3.3:11]
*>i  [3]:[10]:[32,3.3.3.3]
                     3.3.3.3             0         100          0        i  3.3.3.3         VXLAN

RD[3.3.3.3:21]
*>i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0         100          0        i  3.3.3.3         VXLAN

Total number of prefixes 21
```

VTEP3

```
VTEP3#  show nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status Src-Addr         Dst-Addr
_____________________________________________________________________________________________________________
___
10       VNI-RED      L2       NW   ----      ----                         ---- ----      3.3.3.3          2.2.2.2
10       VNI-RED      L2       NW   ----      ----                         ---- ----      3.3.3.3          1.1.1.1
10       VNI-RED      --       AC   xe48      --- Single Homed Port ---    1001 ----      ----             ----
10       VNI-RED      --       AC   xe48      --- Single Homed Port ---    1002 ----      ----             ----
20       VNI-BLUE     L2       NW   ----      ----                         ---- ----      3.3.3.3          2.2.2.2
20       VNI-BLUE     L2       NW   ----      ----                         ---- ----      3.3.3.3          1.1.1.1
20       VNI-BLUE     --       AC   xe48      --- Single Homed Port ---    3001 ----      ----             ----

Total number of entries are 7
```

```
VTEP3#show nvo vxlan access-if brief

                  Inner                       Admin   Link
Interface  Vlan   vlan  Ifindex  Vnid         status  status
-----------------------------------------------------------
xe48       1002   ---   500001   10           up      up
xe48       1001   ---   500000   10           up      up
xe48       3001   ---   500002   20           up      up

Total number of entries are 3
```

```
VTEP3#show bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 500
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd     AD  MACIP  MCAST    ESI
PREFIX-ROUTE
1.1.1.1                 4   500  177       173      3     0      0  01:11:49            6      3     0      2      1      0
2.2.2.2                 4   500  177       171      2     0      0  01:11:59            6      3     0      2      1      0

Total number of neighbors 2

Total number of Established sessions 2
```

```
VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
```

```
Source           Destination      Status           Up/Down        Update
================================================================================
3.3.3.3          2.2.2.2          Installed        01:12:10       01:12:10
3.3.3.3          1.1.1.1          Installed        01:12:00       01:12:00

Total number of entries are 2

VTEP3#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  1.1.1.1         1.1.1.1         VXLAN

RD[2.2.2.2:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN

VTEP3#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN

RD[3.3.3.3:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

VTEP3#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN

RD[2.2.2.2:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             2.2.2.2         VXLAN
```

```
RD[2.2.2.2:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN

RD[3.3.3.3:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   10          10             1.1.1.1         VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   20          20             1.1.1.1         VXLAN

VTEP3#show bgp l2vpn evpn
BGP table version is 4, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[1.1.1.1:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[1.1.1.1:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [3]:[10]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[1.1.1.1:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN
*>i  [3]:[20]:[32,1.1.1.1]
                     1.1.1.1             0         100          0        i  1.1.1.1         VXLAN

RD[2.2.2.2:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     2.2.2.2             0         100          0        i  2.2.2.2         VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                     2.2.2.2             0         100          0        i  2.2.2.2         VXLAN

RD[2.2.2.2:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                     2.2.2.2             0         100          0        i  2.2.2.2         VXLAN
```

```
*>i  [3]:[10]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN

RD[2.2.2.2:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
*>i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN

RD[3.3.3.3:11] VRF[VRF1]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
* i                  1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
* i                  1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [3]:[10]:[32,1.1.1.1]
                    1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [3]:[10]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
*>   [3]:[10]:[32,3.3.3.3]
                    3.3.3.3             0         100           32768    i  ----------      VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
* i                  1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
* i                  1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [3]:[20]:[32,1.1.1.1]
                    1.1.1.1             0         100           0        i  1.1.1.1         VXLAN
* i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2         VXLAN
*>   [3]:[20]:[32,3.3.3.3]
                    3.3.3.3             0         100           32768    i  ----------      VXLAN

Total number of prefixes 22
```

Static MAC-IP Advertise through Single Home and Multihomed VTEPs

Advertise static MAC IPv4 from MH1 and SH3.

MH1-VTEPs: VTEP1 & VTEP2- same MAC should be configured on both VTEPs under po access-port, configs should be symmetric between MH VTEPs

SH3-VTEP: VTEP3

VTEP1 (MH1)

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 1001`	Enter into VxLAN MH po1 access-port with VLAN 1001

(config-nvo-acc-if)#mac 0000.1111.1001 ip 11.11.10.1	Configure static MAC IP
(config-nvo-acc-if)#exit	Exit from VxLAN access-port config mode
(config)#exit	Exit from configuration mode

VTEP2 (MH1)

#configure terminal	Enter Configure mode.
(config)#nvo vxlan access-if port-vlan po1 1001	Enter into VxLAN MH po1 access-port with vlan 1001
(config-nvo-acc-if)# mac 0000.1111.1001 ip 11.11.10.1	Configure static MAC IP
(config-nvo-acc-if)#exit	Exit from VxLAN access-port config mode
(config)#exit	Exit from configuration mode

VTEP3 (SH)

#configure terminal	Enter Configure mode.
(config)# nvo vxlan access-if port-vlan xe48 1001	Enter into single-homed access-port - xe48 with VLAN 1001
(config-nvo-acc-if)#mac 0000.3333.1001 ip 11.11.10.2	Configure static MAC IP
(config-nvo-acc-if)#exit	Exit from VxLAN access-port config mode
(config)#exit	Exit from configuration mode

Validation

Verify MAC-table in MH VTEPs and Single Home VTEP, MAC will be advertised through ESI value which is advertised from VTEP1 and VTEP2 and VTEP IP from SH VTEP VTEP3.

Verify ARP-cache table in all VTEPs, VTEP1 and VTEP2 will learn VTEP3 IP.

Any ARP request comes for 11.11.10.2, VTEP1/VTEP2 will do proxy-ARP.

VTEP1

```
VTEP1#show nvo vxlan mac-table
================================================================================================================================
                                                VXLAN MAC Entries
================================================================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI                  Type           Status     AccessPortDesc
________________________________________________________________________________________________________________________
____________

10         po1       1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00  Static Local    -------    -------
10         ----      ----   ----         0000.3333.1001 3.3.3.3                       Static Remote   -------    -------

Total number of entries are : 2

VTEP1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
```

```
VNID      Ip-Addr           Mac-Addr       Type         Age-Out    Retries-Left
_____________________________________________________________________________
10        11.11.10.1        0000.1111.1001 Static Local   ----
10        11.11.10.2        0000.3333.1001 Static Remote  ----
Total number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan mac-table
================================================================================================================================
                                                VXLAN MAC Entries
================================================================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI                  Type           Status     AccessPortDesc
________________________________________________________________________________________________________________________________

10         po1       1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00  Static Local    -------    -------
10         ----      ----   ----         0000.3333.1001 3.3.3.3                       Static Remote   -------    -------

Total number of entries are : 2
```

```
VTEP2#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID      Ip-Addr           Mac-Addr       Type         Age-Out    Retries-Left
_____________________________________________________________________________
10        11.11.10.1        0000.1111.1001 Static Local   ----
10        11.11.10.2        0000.3333.1001 Static Remote  ----
Total number of entries are 2
```

VTEP3

```
VTEP3#show nvo vxlan mac-table
================================================================================================================================
                                                VXLAN MAC Entries
================================================================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI                  Type           Status     AccessPortDesc
________________________________________________________________________________________________________________________________

10         ----      1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00  Static Remote   -------    -------
10         xe48      1001   ----         0000.3333.1001 3.3.3.3                       Static Local    -------    -------

Total number of entries are : 2
```

```
VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID      Ip-Addr           Mac-Addr       Type         Age-Out    Retries-Left
_____________________________________________________________________________
10        11.11.10.1        0000.1111.1001 Static Remote  ----
10        11.11.10.2        0000.3333.1001 Static Local   ----
Total number of entries are 2
```

Dynamic MAC Advertise through Single Home and Multihomed VTEPs

Advertise 2 MAC's through CE1 connected IXIA, dynamic MAC entries and verify MAC-table in all VTEPs.

One MAC will be dynamic local in VTEP1 and same will be remote in VTEP2 and other be dynamic local in VTEP2 and same will be remote in VTEP1.

Both MAC's will be in remote in VTEP3.

VTEP1

```
VTEP1#show nvo vxlan mac-table
================================================================================================================================
                                                VXLAN MAC Entries
================================================================================================================================
VNID      Interface VlanId Inner-VlanId Mac-Addr      VTEP-Ip/ESI                 Type           Status     AccessPortDesc
--------------------------------------------------------------------------------------------------------------------------------

10        po1       1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00  Dynamic Local   -------    -------
10        ----      1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00  Dynamic Remote  -------    -------

Total number of entries are : 2
```

```
VTEP1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
VNID      Ip-Addr           Mac-Addr        Type         Age-Out    Retries-Left
--------------------------------------------------------------------------------
10        21.21.21.1        0000.1111.1002 Dynamic Local  ----
10        31.1.31.1         0000.1111.1003 Dynamic Remote ----
Total number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan mac-table
================================================================================================================================
                                                VXLAN MAC Entries
================================================================================================================================
VNID      Interface VlanId Inner-VlanId Mac-Addr      VTEP-Ip/ESI                 Type           Status     AccessPortDesc
--------------------------------------------------------------------------------------------------------------------------------

10        ----      1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00  Dynamic Remote  -------    -------
10        po1       1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00  Dynamic Local   -------    -------

Total number of entries are : 2
```

```
VTEP2#show nvo vxla arp-cache
VXLAN ARP-CACHE Information
============================
VNID      Ip-Addr           Mac-Addr        Type         Age-Out    Retries-Left
--------------------------------------------------------------------------------
10        21.21.21.1        0000.1111.1002 Dynamic Remote ----
10        31.1.31.1         0000.1111.1003 Dynamic Local  ----
Total number of entries are 2
```

VTEP3

```
VTEP3#show nvo vxlan mac-table
================================================================================================================================
==============
                                                VXLAN MAC Entries
================================================================================================================================
==============
VNID      Interface VlanId Inner-VlanId Mac-Addr      VTEP-Ip/ESI                 Type           Status     AccessPortDesc
--------------------------------------------------------------------------------------------------------------------------------
--------------

10        ----      1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00  Dynamic Remote  -------    -------
10        ----      1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00  Dynamic Remote  -------    -------
```

```
Total number of entries are : 2

VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       21.21.21.1       0000.1111.1002 Dynamic Remote ----
10       31.1.31.1        0000.1111.1003 Dynamic Remote ----
Total number of entries are 2
```

Note:

- When VTEP1 tunnel goes down, then traffic from VTEP3 will use VTEP2 for forwarding. But Traffic from Switch to VTEP1 will be lost in VTEP1 itself.
- When DUT is rebooted, access-if will be in hold down state until ESI hold timer value expiry. After ESI hold timer expiry, access-if port will be up and started learning.
- MAC Hold timer will not be applicable on ESI interface, because of mass-withdraw requirement.
- A CE can connect to maximum two nodes for multihoming, more than two nodes in a multihoming group is not supported.
- All configuration (shutdown, disable learning, disable arp/nd cache, disable arp/nd flood, map vnid, qos profiles, encapsulation) on a multihomed access port should be same on both VTEPs sharing the ESI for multihoming functionalities to work properly.
- Multiple ESI values are supported on same VTEP.

CHAPTER 4 VXLAN Quality of Service Configuration

This chapter contains the configurations for VXLAN Quality of Service (QoS).

Overview

VXLAN enables multiple tenants to operate in a data center. Each tenant is assigned a priority group to prioritize their traffic. Cloud carriers want to use quality of service to differentiate different applications.

Data center networks are being increasingly used by telecommunications operators as well as by enterprises. Currently these networks are organized as one large Layer 2 network in a single building. In some cases, such a network is extended geographically using Virtual Local Area Network (VLAN) technologies as an even larger Layer 2 network connecting the virtual machines (VM), each with its own MAC address.

Multiple tenants might want their own isolated network domain. In a data center hosting multiple tenants, each tenant may independently assign MAC addresses and VLAN IDs and this might lead to duplication.

Cloud carriers wish to categorize the traffic based on the application such as voice, video, etc. Based on the type of the application different traffic classes may be identified and different priority levels can be assigned to each. To do so, quality of service marking is needed in VXLAN.

This chapter shows how to mark packet headers with the VXLAN tunnel end point (VTEP) when the frames are introduced by the virtual machines. The (re)marking /setting of QoS field DSCP/TOS in the VXLAN IP header is done with the two modes which are set globally.

Topology

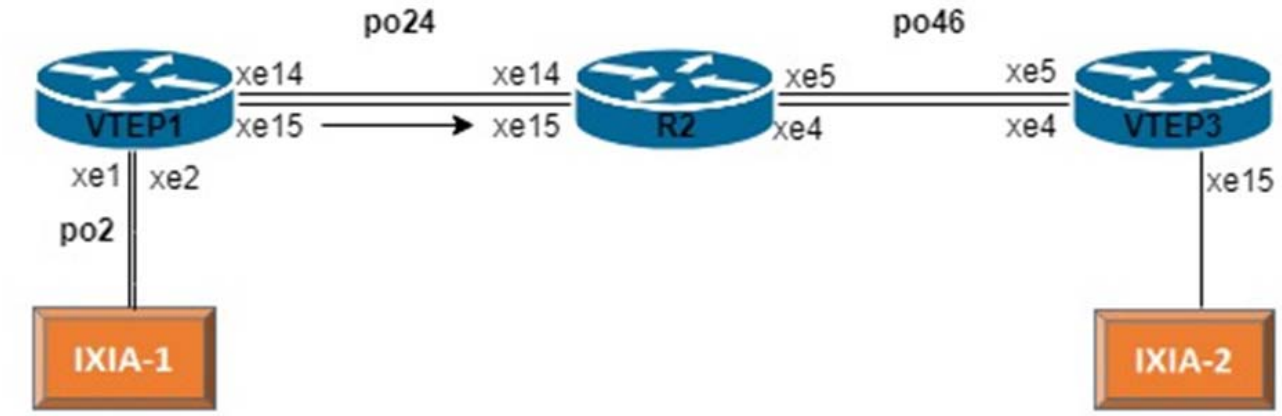


Figure 4-129: VXLAN QoS

COS-DSCP

RTR1/VTEP1

`VTEP1#configure terminal`	Enter Configure mode.
`VTEP1(config)#mac vrf vrf1`	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
`VTEP1(config-vrf)#rd 1.1.1.1:11`	Assign RD value
`VTEP1(config-vrf)#route-target both 10.10.10.10:100`	Assign route-target value for import/export
`VTEP1(config-vrf)#hardware-profile filter vxlan enable`	Enable hardware profile for vxlan
`VTEP1(config)#nvo vxlan enable`	Enable vxlan
`VTEP1(config)#qos enable`	Enable qos
`VTEP1(config)#qos profile cos-to-queue COS-QUE`	Create qos profile for mapping traffic towards tunnel from access-if.
`VTEP1(config-ingress-cos-map)#cos 1 queue 3`	Configure particular COS value to the queue value for configured profile.
`VTEP1(config-ingress-dscp-map)#qos profile queue-color-to-dscp QUE-DSCP`	Create qos profile for attaching in vxlan tunnel egress.
`VTEP1(config-egress-dscp-map)#queue 3 dscp 16`	Configure particular queue value to the dscp value for configured profile.
`VTEP1(config-egress-dscp-map)#interface po2`	Create a port channel po2
`VTEP1(config-if)#switchport`	Configure port as switchport
`VTEP1(config-if)#load-interval 30`	Set load-interval
`VTEP1(config-if)#interface po24`	Create a port channel po24
`VTEP1(config-if)#load-interval 30`	Configure port as switchport
`VTEP1(config-if)#ip address 24.1.1.1/30`	Set load-interval
`VTEP1(config-if)#interface lo`	Enter in to loopback interface
`VTEP1(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address
`VTEP1(config-if)#interface xe1`	Enter in to interface mode
`VTEP1(config-if)#channel-group 2 mode active`	Map to channel-group
`VTEP1(config-if)#interface xe2`	Enter in to interface mode
`VTEP1(config-if)#channel-group 2 mode active`	Map to channel-group
`VTEP1(config-if)#interface xe14`	Enter in to interface mode
`VTEP1(config-if)#channel-group 24 mode active`	Map to channel-group
`VTEP1(config-if)#interface xe15`	Enter in to interface mode
`VTEP1(config-if)#channel-group 24 mode active`	Map to channel-group
`VTEP1(config-if)#router ospf 1`	Create ospf instance
`VTEP1(config-router)#ospf router-id 1.1.1.1`	Configure ospf router-id

VTEP1(config-router)#network 1.1.1.1/32 area 0.0.0.0	Configure loopback network address in to ospf
VTEP1(config-router)#network 24.1.1.0/30 area 0.0.0.0	Configure network address in to ospf
VTEP1(config-router)#router bgp 100	Enter into Router BGP mode
VTEP1(config-router)#neighbor 6.6.6.6 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
VTEP1(config-router)#neighbor 6.6.6.6 update-source lo	Specify the neighbor to use loopback address as source
VTEP1(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address-family
VTEP1(config-router-af)#neighbor 6.6.6.6 activate	Activate the neighbor to address-family
VTEP1(config-router)#nvo vxlan vtep-ip-global 1.1.1.1	Configure Source vtep-ip-global configuration
VTEP1(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress QUE-DSCP	Configure the mapping qos profile in to vxlan tunnel egress
VTEP1(config)#nvo vxlan id 1 in-gress-replication inner-vid-disabled	Create vnid 1 and disable inner-vid
VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
VTEP1(config-nvo)#nvo vxlan access-if port-vlan po2 1001	Create vxlan access-if with vlan 1001
VTEP1(config-nvo-acc-if)#no shutdown	No shut the vxlan access-if
VTEP1(config-nvo-acc-if)#map vnid 1	Map vnid to the vxlan access-if
VTEP1(config-nvo-acc-if)#map qos-profile cos-to-queue COS-QUE	Map qos profile for vxlan access-if ingress traffic from CE

RTR2

R2#configure terminal	Enter Configure mode.
R2(config)#interface po24	Create port channel
R2(config-if)#load-interval 30	Set load-interval
R2(config-if)#ip address 24.1.1.2/30	Assign ip address
R2(config-if)#interface po46	Create port channel
R2(config-if)#load-interval 30	Set load-interval
R2(config-if)#ip address 46.1.1.1/30	Assign ip address
R2(config-if)#interface lo	Enter in to loopback interface
R2(config-if)#ip address 4.4.4.4/32 secondary	Assign secondary ip address
R2(config-if)#interface xe4	Enter into interface mode
R2(config-if)#channel-group 46 mode active	Map port channel to the interface
R2(config-if)#interface xe5	Enter into interface mode
R2(config-if)#channel-group 46 mode active	Map port channel to the interface
R2(config-if)#interface xe14	Enter into interface mode
R2(config-if)#channel-group 24 mode active	Map port channel to the interface

`R2(config-if)#interface xe15`	Enter into interface mode
`R2(config-if)#channel-group 24 mode active`	Map port channel to the interface
`R2(config-if)#router ospf 1`	Create ospf instance
`R2(config-router)#ospf router-id 4.4.4.4`	Configure ospf router-id
`R2(config-router)#network 4.4.4.4/32 area 0.0.0.0`	Configure ospf network address with respective area
`R2(config-router)#network 24.1.1.0/30 area 0.0.0.0`	Configure ospf network address with respective area
`R2(config-router)#network 46.1.1.0/30 area 0.0.0.0`	Configure ospf network address with respective area

RTR3/VTEP2

`VTEP3#configure terminal`	Enter Configuration mode
`VTEP3(config)#mac vrf vrf1`	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
`VTEP3(config-vrf)#rd 6.6.6.6:11`	Assign RD value
`VTEP3(config-vrf)#route-target both 10.10.10.10:100`	Assign route-target value for import/export
`VTEP3(config-vrf)#hardware-profile filter vxlan enable`	Enable hardware profile vxlan
`VTEP3(config)#nvo vxlan enable`	Enable vxlan
`VTEP3(config)#qos enable`	Enable QOS
`VTEP3(config)#qos statistics`	Enable QOS statistics
`VTEP3(config-ingress-cos-map)#qos profile queue-color-to-cos QUE-COS`	Create qos profile for mapping incoming traffic from tunnel to access-if.
`VTEP3(config-egress-cos-map)#queue 4 cos 5`	Configure particular queue value to the cos value for configured profile.
`VTEP3(config-egress-cos-map)#qos profile dscp-to-queue DSCP-QUE`	Create qos profile for attaching in vxlan tunnel ingress.
`VTEP3(config-ingress-dscp-map)#dscp 16 queue 4`	Configure particular dscp value to the queue value for configured profile.
`VTEP3(config-egress-dscp-map)#interface po46`	Create port channel
`VTEP3(config-if)#load-interval 30`	Set load interval
`VTEP3(config-if)#ip address 46.1.1.2/30`	Assign ip address
`VTEP3(config-if)#interface lo`	Enter into loopback interface
`VTEP3(config-if)#ip address 6.6.6.6/32 secondary`	Assign secondary ip address
`VTEP3(config-if)#interface xe4`	Enter into interface mode
`VTEP3(config-if)#channel-group 46 mode active`	Map channel group into the interface
`VTEP3(config-if)#interface xe5`	Enter into interface mode
`VTEP3(config-if)#channel-group 46 mode active`	Map channel group into the interface
`VTEP3(config-if)#interface xe15`	Enter into interface mode

VTEP3(config-if)#switchport	Make interface as L2 port
VTEP3(config-if)#load-interval 30	Set load interval
VTEP3(config-if)#router ospf 1	Create ospf instance
VTEP3(config-router)#ospf router-id 6.6.6.6	Configure ospf router-id
VTEP3(config-router)#network 6.6.6.6/32 area 0.0.0.0	Configure ospf network address with respective area
VTEP3(config-router)#network 46.1.1.0/30 area 0.0.0.0	Configure ospf network address with respective area
VTEP3(config-router)#router bgp 100	Enter into Router BGP mode
VTEP3(config-router)#neighbor 1.1.1.1 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
VTEP3(config-router)#neighbor 1.1.1.1 update-source lo	Specify the neighbor to use loopback address as source
VTEP3(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address-family
VTEP3(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor to address-family
VTEP3(config)#nvo vxlan vtep-ip-global 6.6.6.6	Configure Source vtep-ip-global configuration
VTEP3(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress DSCP-QUE	Configure the mapping qos profile in to vxlan tunnel ingress
VTEP3(config)#nvo vxlan id 1 in-gress-replication inner-vid-disabled	Create vnid 1 and disable inner-vid
VTEP3(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
VTEP3(config-nvo)#nvo vxlan access-if port-vlan xe15 1000	Create vxlan access-if with vlan 1000
VTEP3(config-nvo-acc-if)#no shutdown	No shut the vxlan access-if
VTEP3(config-nvo-acc-if)#map vnid 1	Map vnid to the vxlan access-if
VTEP3(config-nvo-acc-if)#map qos-profile queue-color-to-cos QUE-COS	Map qos profile for vxlan access-if egress traffic to CE

Validation

RTR1/VTEP1

```
VTEP1#sh run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 1.1.1.1
!
nvo vxlan tunnel qos-map-mode cos-dscp egress QUE-DSCP
!
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
```

```
nvo vxlan access-if port-vlan po2 1001
 no shutdown
 map vnid 1
 map qos-profile cos-to-queue COS-QUE
!
VTEP1#show run qos
qos enable
!
qos profile cos-to-queue COS-QUE
 cos 2 queue 3
!
qos profile queue-color-to-dscp QUE-DSCP
 queue 3 dscp 16
!

VTEP1#sh int xe14 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
q0                (E) 12517376 0                 0                   0                 0
q1                (E) 12517376 0                 0                   0                 0
q2                (E) 12517376 0                 0                   0                 0
q3                (E) 12517376 205284588         188040683524        0                 0
q4                (E) 12517376 0                 0                   0                 0
q5                (E) 12517376 0                 0                   0                 0
q6                (E) 12517376 0                 0                   0                 0
q7                (E) 12517376 7518              1007412             0                 0

VTEP1#sh int xe15 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
q0                (E) 12517376 0                 0                   0                 0
q1                (E) 12517376 0                 0                   0                 0
q2                (E) 12517376 0                 0                   0                 0
q3                (E) 12517376 205624494         188352040168        0                 0
q4                (E) 12517376 0                 0                   0                 0
q5                (E) 12517376 0                 0                   0                 0
q6                (E) 12517376 0                 0                   0                 0
q7                (E) 12517376 9006              1136741             0                 0

VTEP1#
VTEP1#show nvo vxlan
VXLAN Information
```

```
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name    VNI-Type Type Interface ESI                           VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
1       ----        L2      NW   ----     ----                           ---- ----
1.1.1.1          6.6.6.6
1      ----       AC   po2      --- Single Hommed port ---   1001 ----     ----
----

Total number of entries are 3
VTEP1#show nvo vxlan mac-table
=============================================================================================
============================================================
                                                                VXLAN MAC Entries
=============================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
_____________________________________________________________________________________
_____________________________________________________

1         po2        1001   ----         0000.2000.9991 1.1.1.1
Dynamic Local        -------             -------

Total number of entries are : 1

VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
1.1.1.1          6.6.6.6          Installed        00:11:29        00:11:29

Total number of entries are 2
VTEP1#
```

RTR3/VTEP3

```
VTEP3#show run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 6.6.6.6
!
nvo vxlan tunnel qos-map-mode cos-dscp ingress DSCP-QUE
!
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
```

```
nvo vxlan access-if port-vlan xe15 1000
 no shutdown
 map vnid 1
 map qos-profile queue-color-to-cos QUE-COS
!
!
VTEP3#sh run qos
qos enable
qos statistics
!
qos profile queue-color-to-cos QUE-COS
 queue 4 cos 5
!
qos profile dscp-to-queue DSCP-QUE
 dscp 16 queue 4
!
VTEP3#show nvo vxlan mac-table

================================================================================================
================================================================
                                                                VXLAN MAC Entries
================================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
------------------------------------------------------------------------------------------------
------------------------------------------------------------------

1         ----       ----   ----         0000.2000.9991 1.1.1.1
Dynamic Remote       -------             -------

Total number of entries are : 1

VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
6.6.6.6          1.1.1.1          Installed       00:09:39        00:09:39

Total number of entries are 2
VTEP3#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name     VNI-Type Type Interface ESI                           VLAN DF-Status
Src-Addr         Dst-Addr
------------------------------------------------------------------------------------------------
----------------------------------------
```

```
1       ----         L2      NW   ----      ----                          ---- ----
6.6.6.6          1.1.1.1
1      ----       AC   xe15     --- Single Hommed port ---    1000 ----     ----
----

Total number of entries are 3
VTEP3#

VTEP3#show int xe15 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------
+-------------------+
q0                (E) 12517376 0                 0                   0                 0
q1                (E) 12517376 0                 0                   0                 0
q2                (E) 12517376 0                 0                   0                 0
q3                (E) 12517376 0                 0                   0                 0
q4                (E) 12517376 37895872          36455829826         0                 0
q5                (E) 12517376 0                 0                   0                 0
q6                (E) 12517376 0                 0                   0                 0
q7                (E) 12517376 0                 0                   0                 0

VTEP3#
```

CHAPTER 5 VXLAN Tunnel Over SVI

This chapter contains the configurations for VXLAN Tunnel Over SVI.

Overview

VxLAN EVPN solution is envisioned to simplify the topology and configurations in Data Centers (DC). In Data Centers, CLOS topology was used, which makes network side pure L3 and uses EBGP as IGP.

VxLAN solution is required for Service Providers (SP) as well to run few of the services or all services in their network over VxLAN. When they choose to run few services over VxLAN, then on the network side there will be a need to run VxLAN over SVI.

Topology

The Topology shown below contains the 3 VTEPS i.e VTEP1 ,VTEP2 and VTEP3 and 3 core nodes P1 ,P2 and P3. Vxlan tunnel will be established between VTEPS over SVI interfaces. OSPF as IGP will be running between VTEPS and the core node to provide the end to end connectivity. Switch is connected between host and VTEP-1, VTEP-2 via dynamic LAG.

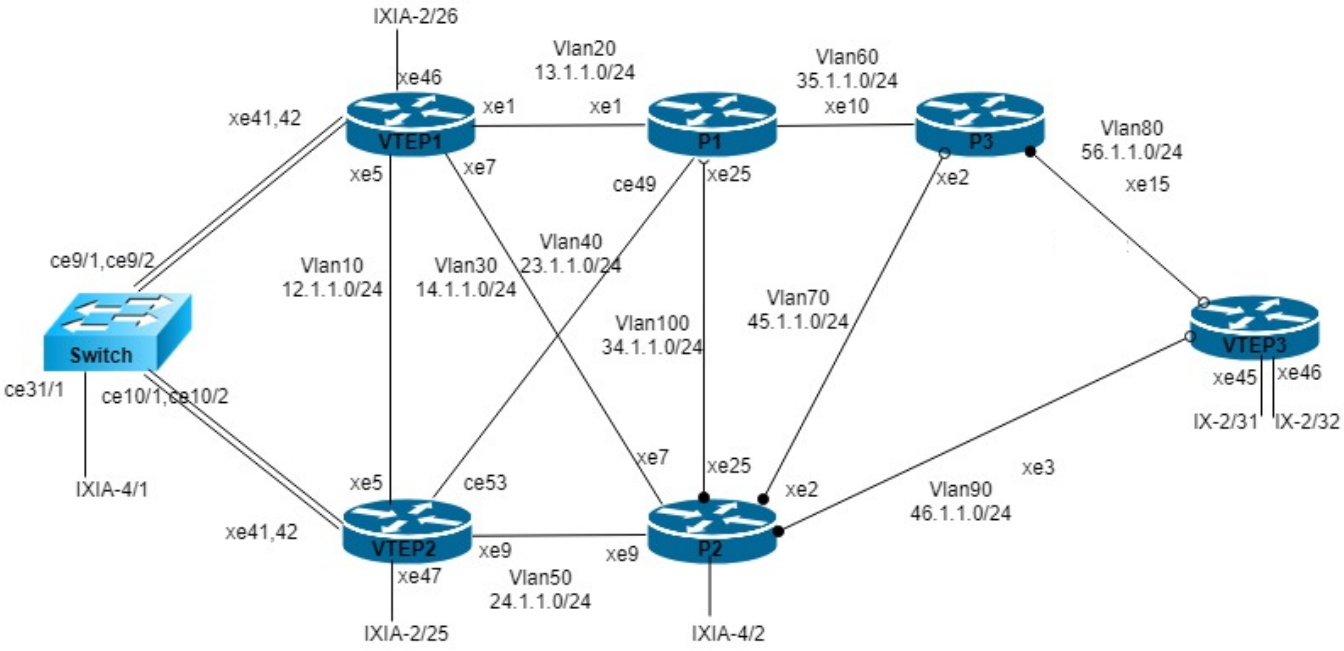


Figure 5-130: VXLAN over SVI

RTR1/VTEP1

`VTEP1#configure terminal`	Enter configuration terminal
`VTEP1(config)#hostname VTEP1`	Configure hostname

`VTEP1(config)#mac vrf vrf1`	Configure mac vrf vrf1
`VTEP1(config-vrf)# rd 1.1.1.1:11`	Configure RD for vrf1
`VTEP1(config-vrf)# route-target both 10.10.10.10:100`	Configure RT for vrf1
`VTEP1(config-vrf)#mac vrf vrf2`	Configure mac vrf vrf2
`VTEP1(config-vrf)# rd 1.1.1.1:12`	Configure RD for vrf2
`VTEP1(config-vrf)# route-target both 10.10.10.10:102`	Configure RT for vrf2
`VTEP1(config-vrf)#bfd interval 3 minrx 3 multiplier 3`	Configure bfd interval globally
`VTEP1(config)#hardware-profile filter egress-ipv4 enable`	Enable hardware filter for egress ipv4
`VTEP1(config)#hardware-profile filter vxlan enable`	Enable vxlan in hardware
`VTEP1(config)#nvo vxlan enable`	Enable vxlan
`VTEP1(config)#qos enable`	Enable qos
`VTEP1(config)#qos statistics`	Enable qos statistics
`VTEP1(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE vlan bridge
`VTEP1(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`VTEP1(config)#no igmp snooping`	Disable igmp snooping messages globally
`VTEP1(config)#vlan database`	Enter into the vlan database
`VTEP1(config-vlan)# vlan 10-200 bridge 1 state enable`	Configure vlan 10-200 and associate with bridge 1
`VTEP1(config-vlan)# vlan 4000 bridge 1 state enable`	Configure vlan 4000 and associate with bridge 1
`VTEP1(config-vlan)#interface po1`	Enter interface mode
`VTEP1(config-if)# switchport`	Set the interface as Layer2 port
`VTEP1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP1(config-if)#interface lo`	Enter lo interface mode
`VTEP1(config-if)# ip address 1.1.1.1/32 secondary`	Assign loopback ip
`VTEP1(config-if)#interface vlan1.10`	Specify interface vlan1.10 to be configured.
`VTEP1(config-if)# ip address 12.1.1.1/24`	Assign ip address
`VTEP1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`VTEP1(config-if)#interface vlan1.20`	Specify interface vlan1.20 to be configured.
`VTEP1(config-if)# ip address 13.1.1.1/24`	Assign ip address
`VTEP1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`VTEP1(config-if)#interface vlan1.30`	Specify interface vlan1.30 to be configured.
`VTEP1(config-if)# ip address 14.1.1.1/24`	Assign ip address
`VTEP1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`VTEP1(config-if)#interface vlan1.110`	Specify interface vlan1.110 to be configured.
`VTEP1(config-if)# ip address 15.1.1.1/24`	Assign ip address

VTEP1(config-if)# ip ospf cost 1	Change ospf cost of the link
VTEP1(config-if)#interface xe1	Enter interface mode
VTEP1(config-if)# switchport	Set the interface as Layer2 port
VTEP1(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)# switchport trunk allowed vlan add 20,29	Enable VLAN's allowed on this interface.
VTEP1(config-if)# switchport trunk native vlan 29	Configure native vlan
VTEP1(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe5	Enter interface mode
VTEP1(config-if)# switchport	Set the interface as Layer2 port
VTEP1(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)# switchport trunk allowed vlan add 10-19	Enable VLAN's allowed on this interface.
VTEP1(config-if)# switchport trunk native vlan 19	Configure native vlan
VTEP1(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe7	Enter interface mode
VTEP1(config-if)# switchport	Set the interface as Layer2 port
VTEP1(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)# switchport trunk allowed vlan add 30,39	Enable VLAN's allowed on this interface.
VTEP1(config-if)# switchport trunk native vlan 39	Configure native vlan
VTEP1(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe19	Enter interface mode
VTEP1(config-if)# switchport	Set the interface as Layer2 port
VTEP1(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)# switchport trunk allowed vlan add 110-111	Enable VLAN's allowed on this interface.
VTEP1(config-if)# switchport trunk native vlan 111	Configure native vlan

`VTEP1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP1(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP1(config-if)#interface xe41`	Enter interface mode
`VTEP1(config-if)# channel-group 1 mode active`	Map this interface to po1
`VTEP1(config-if)#interface xe46`	Enter interface mode
`VTEP1(config-if)# switchport`	Map this interface to po1
`VTEP1(config-if)#router ospf 1`	Enter ospf configuration mode
`VTEP1(config-router)# ospf router-id 1.1.1.1`	Configure ospf router id
`VTEP1(config-router)# bfd all-interfaces`	Enable bfd in all ospf interfaces
`VTEP1(config-router)# network 1.1.1.1/32 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)# network 12.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)# network 13.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)# network 14.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)# network 15.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)#router bgp 100`	Enter Router BGP mode and define the AS number 100.
`VTEP1(config-router)# network 1.1.1.1/32`	Add the lo network to bgp route
`VTEP1(config-router)# neighbor 2.2.2.2 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`VTEP1(config-router)# neighbor 2.2.2.2 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP1(config-router)# neighbor 6.6.6.6 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`VTEP1(config-router)# neighbor 6.6.6.6 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP1(config-router)# address-family l2vpn evpn`	Enter in to bgp l2vpn evpn address-family
`VTEP1(config-router-af)# neighbor 2.2.2.2 activate`	Activate neigbors
`VTEP1(config-router-af)# neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP1(config-router-af)# exit-address-family`	Exit from bgp l2vpn evpn address-family
`VTEP1(config-router)#nvo vxlan vtep-ip-global 1.1.1.1`	Configure vxlan global ip
`VTEP1(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Create vnid 1
`VTEP1(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf1`	Associate vnid with evpn and vrf1
`VTEP1(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled`	Create vnid 1000
`VTEP1(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf2`	Associate vnid with evpn and vrf2

VTEP1(config-nvo)#nvo vxlan access-if port xe46	Create vxlan access port
VTEP1(config-nvo-acc-if)# no shutdown	Unshut the access interface
VTEP1(config-nvo-acc-if)# map vnid 1000	Map the vnid to access-if
VTEP1(config-nvo-acc-if)#nvo vxlan access-if port-vlan po1 1000	Create vxlan access port port-vlan
VTEP1(config-nvo-acc-if)# no shutdown	Unshut the access interface
VTEP1(config-nvo-acc-if)# map vnid 1	Map the vnid to access-if
VTEP1(config-nvo-acc-if)# mac 0000.1111.1111 ip 100.1.1.100	Configure static mac ip
VTEP1(config-nvo-acc-if)# mac 0000.1111.1112	Configure static mac
VTEP1(config-nvo-acc-if)# mac 0000.1111.1113	Configure static mac
VTEP1(config-nvo-acc-if)# mac 0000.1111.1114	Configure static mac
VTEP1(config-nvo-acc-if)# mac 0000.1111.1115	Configure static mac

VTEP2

VTEP2#configure terminal	Enter configuration terminal
VTEP2(config)#hostname VTEP2	Configure hostname
VTEP2(config)#mac vrf vrf1	Configure mac vrf vrf1
VTEP2(config-vrf)# rd 2.2.2.2:11	Configure RD for vrf1
VTEP2(config-vrf)# route-target both 10.10.10.10:100	Configure RT for vrf1
VTEP2(config-vrf)#mac vrf vrf2	Configure mac vrf vrf2
VTEP2(config-vrf)# rd 2.2.2.2:12	Configure RD for vrf2
VTEP2(config-vrf)# route-target both 10.10.10.10:102	Configure RT for vrf2
VTEP2(config-vrf)#load-balance enable	Enable load balancing
VTEP2(config)#load-balance l2 dest-mac src-mac	Enable load balance based on mac address
VTEP2(config)#load-balance ipv4 dest-ipv4 src-ipv4	Enable load balance based on ip address
VTEP2(config)#hardware-profile filter egress-ipv4 enable	Enable hardware filter for egress ipv4
VTEP2(config)#hardware-profile filter vxlan enable	Enable vxlan in hardware
VTEP2(config)#nvo vxlan enable	Enable vxlan
VTEP2(config)#qos enable	Enable qos
VTEP2(config)#qos statistics	Enable qos statistics
VTEP2(config)#bridge 1 protocol ieee vlan-bridge	Configure IEEE vlan bridge
VTEP2(config)#no bridge 1 spanning-tree enable	Disable spanning tree in bridge 1 globally
VTEP2(config)#vlan database	Enter into the vlan database

`VTEP2(config-vlan)# vlan 10-200 bridge 1 state enable`	Configure vlan 10-200 and associate with bridge 1
`VTEP2(config-vlan)#interface po2`	Enter interface mode
`VTEP2(config-if)# switchport`	Set the interface as Layer2 port
`VTEP2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)#interface ce53`	Enter interface mode
`VTEP2(config-if)# switchport`	Set the interface as Layer2 port
`VTEP2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`VTEP2(config-if)# switchport trunk allowed vlan add 40,49`	Enable VLAN's allowed on this interface.
`VTEP2(config-if)# switchport trunk native vlan 49`	Configure native vlan
`VTEP2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP2(config-if)#interface lo`	Enter interface mode
`VTEP2(config-if)# ip address 2.2.2.2/32 secondary`	Configure loopback ip
`VTEP2(config-if)#interface vlan1.10`	Specify interface vlan1.10 to be configured.
`VTEP2(config-if)# ip address 12.1.1.2/24`	Assign ip address
`VTEP2(config-if)#interface vlan1.40`	Specify interface vlan1.40 to be configured.
`VTEP2(config-if)# ip address 23.1.1.1/24`	Assign ip address
`VTEP2(config-if)# ip ospf cost 1`	Change ospf cost of the link
`VTEP2(config-if)#interface vlan1.50`	Specify interface vlan1.50 to be configured.
`VTEP2(config-if)# ip address 24.1.1.1/24`	Assign ip address
`VTEP2(config-if)#interface xe5`	Enter interface mode
`VTEP2(config-if)# switchport`	Set the interface as Layer2 port
`VTEP2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`VTEP2(config-if)# switchport trunk allowed vlan add 10-19`	Enable VLAN's allowed on this interface.
`VTEP2(config-if)# switchport trunk native vlan 19`	Configure native vlan
`VTEP2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP2(config-if)#interface xe9`	Enter interface mode
`VTEP2(config-if)# switchport`	Set the interface as Layer2 port
`VTEP2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.

VTEP2(config-if)# switchport trunk allowed vlan add 50,59	Enable VLAN's allowed on this interface.
VTEP2(config-if)# switchport trunk native vlan 59	Configure native vlan
VTEP2(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP2(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP2(config-if)#interface xe12	Enter interface mode
VTEP2(config-if)# switchport	Set the interface as Layer2 port
VTEP2(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP2(config-if)# switchport trunk allowed vlan add 50,59	Enable VLAN's allowed on this interface.
VTEP2(config-if)# switchport trunk native vlan 59	Configure native vlan
VTEP2(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP2(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP2(config-if)#interface xe32	Enter interface mode
VTEP2(config-if)# switchport	Set the interface as Layer2 port
VTEP2(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP2(config-if)# switchport trunk allowed vlan add 160,169	Enable VLAN's allowed on this interface.
VTEP2(config-if)# switchport trunk native vlan 169	Configure native vlan
VTEP2(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
VTEP2(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP2(config-if)#interface xe41	Enter interface mode
VTEP2(config-if)# channel-group 2 mode active	Map the interface to po2
VTEP2(config-if)#interface xe42	Enter interface mode
VTEP2(config-if)# channel-group 2 mode active	Map the interface to po2
VTEP2(config-if)#interface xe47	Enter interface mode
VTEP2(config-if)# switchport	Set the interface as Layer2 port
VTEP2(config-if)#router ospf 1	Enter ospf configuration mode
VTEP2(config-router)# ospf router-id 2.2.2.2	Configure ospf router id
VTEP2(config-router)# network 2.2.2.2/32 area 0.0.0.0	Enable bfd in all ospf interfaces
VTEP2(config-router)# network 12.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
VTEP2(config-router)# network 23.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.

`VTEP2(config-router)# network 24.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)# network 25.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)#router bgp 100`	Enter Router BGP mode and define the AS number 100.
`VTEP2(config-router)# neighbor 1.1.1.1 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`VTEP2(config-router)# neighbor 1.1.1.1 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP2(config-router)# neighbor 6.6.6.6 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`VTEP2(config-router)# neighbor 6.6.6.6 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP2(config-router)# address-family l2vpn evpn`	Enter in to bgp l2vpn evpn address-family
`VTEP2(config-router-af)# neighbor 1.1.1.1 activate`	Activate neigbors
`VTEP2(config-router-af)# neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP2(config-router-af)# exit-address-family`	Exit from bgp l2vpn evpn address-family
`VTEP2(config-router)#nvo vxlan vtep-ip-global 2.2.2.2`	Configure vxlan global ip
`VTEP2(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Create vnid 1
`VTEP2(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf1`	Associate vnid with evpn and vrf1
`VTEP2(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled`	Create vnid 1000
`VTEP2(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf2`	Associate vnid with evpn and vrf2
`VTEP2(config-nvo)#nvo vxlan access-if port xe47`	Create vxlan access port
`VTEP2(config-nvo-acc-if)# no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)# map vnid 1`	Map the vnid to access-if
`VTEP2(config-nvo-acc-if)#nvo vxlan access-if port-vlan po2 2001`	Create vxlan access port
`VTEP2(config-nvo-acc-if)# no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)# map vnid 1000`	Map the vnid to access-if
`VTEP2(config-nvo-acc-if)#nvo vxlan access-if port-vlan po2 2000`	Create vxlan access port
`VTEP2(config-nvo-acc-if)# no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)# map vnid 1000`	Map the vnid to access-if
`VTEP2(config-nvo-acc-if)#end`	Exit from config mode

P1

`P1#configure terminal`	Enter configuration terminal
`P1(config)#hostname P1`	Configure hostname
`P1(config)#bfd interval 3 minrx 3 multiplier 3`	Configure bfd interval globally
`P1(config)#qos enable`	Enable qos
`P1(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE vlan bridge
`P1(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`P1(config)#no igmp snooping`	Disable igmp snooping messages globally
`P1(config)#vlan database`	Enter into the vlan database
`P1(config-vlan)# vlan 10-200 bridge 1 state enable`	Configure vlan 10-200 and associate with bridge 1
`P1(config-vlan)#interface ce49`	Enter interface mode
`P1(config-if)# switchport`	Set the interface as Layer2 port
`P1(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P1(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P1(config-if)# switchport trunk allowed vlan add 40,49`	Enable VLAN's allowed on this interface.
`P1(config-if)# switchport trunk native vlan 49`	Configure native vlan
`P1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P1(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P1(config-if)#interface lo`	Enter loopback interface mode
`P1(config-if)# ip address 3.3.3.3/32 secondary`	Assign loopback ip
`P1(config-if)#interface vlan1.20`	Specify interface vlan1.20 to be configured.
`P1(config-if)# ip address 13.1.1.2/24`	Assign ip address
`P1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P1(config-if)#interface vlan1.40`	Specify interface vlan1.40 to be configured.
`P1(config-if)# ip address 23.1.1.2/24`	Assign ip address
`P1(config-if)#interface vlan1.60`	Specify interface vlan1.60 to be configured.
`P1(config-if)# ip address 35.1.1.1/24`	Assign ip address
`P1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P1(config-if)#interface vlan1.100`	Specify interface vlan1.100 to be configured.
`P1(config-if)# ip address 34.1.1.1/24`	Assign ip address
`P1(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P1(config-if)#interface vlan1.120`	Specify interface vlan1.120 to be configured.
`P1(config-if)# ip address 10.10.10.1/24`	Assign ip address
`P1(config-if)# ip ospf cost 1`	Change ospf cost of the link

`P1(config-if)#interface xe1`	Enter interface mode
`P1(config-if)# switchport`	Set the interface as Layer2 port
`P1(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P1(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P1(config-if)# switchport trunk allowed vlan add 20,29`	Enable VLAN's allowed on this interface.
`P1(config-if)# switchport trunk native vlan 29`	Configure native vlan
`P1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P1(config-if)# mtu 1600`	Change the interface mtu value
`P1(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P1(config-if)#interface xe10`	Enter interface mode
`P1(config-if)# switchport`	Set the interface as Layer2 port
`P1(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P1(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P1(config-if)# switchport trunk allowed vlan add 60,69`	Enable VLAN's allowed on this interface.
`P1(config-if)# switchport trunk native vlan 69`	Configure native vlan
`P1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P1(config-if)# mtu 1600`	Change the interface mtu value
`P1(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P1(config-if)#interface xe25`	Enter interface mode
`P1(config-if)# switchport`	Set the interface as Layer2 port
`P1(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P1(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P1(config-if)# switchport trunk allowed vlan add 100,109`	Enable VLAN's allowed on this interface.
`P1(config-if)# switchport trunk native vlan 109`	Configure native vlan
`P1(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P1(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P1(config-if)#router ospf 1`	Enter ospf configuration mode
`P1(config-router)# ospf router-id 3.3.3.3`	Configure ospf router id
`P1(config-router)# bfd all-interfaces`	Enable bfd in all ospf interfaces
`P1(config-router)# network 3.3.3.3/32 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)# network 10.10.10.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.

P1(config-router)# network 13.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P1(config-router)# network 23.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P1(config-router)# network 34.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P1(config-router)# network 35.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P1(config-router)#end	Exit from config mode

P2

P2#configure terminal	Enter configuration terminal
P2(config)#bfd interval 3 minrx 3 multiplier 3	Configure bfd interval globally
P2(config)#qos enable	Enable qos
P2(config)#hostname P2	Configure hostname
P2(config)#bridge 1 protocol ieee vlan-bridge	Configure IEEE vlan bridge
P2(config)#no bridge 1 spanning-tree enable	Disable spanning tree in bridge 1 globally
P2(config)#no igmp snooping	Disable igmp snooping messages globally
P2(config)#vlan database	Enter into the vlan database
P2(config-vlan)# vlan 10-200 bridge 1 state enable	Configure vlan 10-200 and associate with bridge 1
P2(config-vlan)#interface lo	Enter lo interface mode
P2(config-if)# ip address 4.4.4.4/32 secondary	Assign loopback ip
P2(config-if)#interface vlan1.30	Specify interface vlan1.30 to be configured.
P2(config-if)# ip address 14.1.1.2/24	Assign ip address
P2(config-if)# ip ospf cost 1	Change ospf cost of the link
P2(config-if)#interface vlan1.50	Specify interface vlan1.50 to be configured.
P2(config-if)# ip address 24.1.1.2/24	Assign ip address
P2(config-if)#interface vlan1.70	Specify interface vlan1.70 to be configured.
P2(config-if)# ip address 45.1.1.1/24	Assign ip address
P2(config-if)# ip ospf cost 1	Change ospf cost of the link
P2(config-if)#interface vlan1.90	Specify interface vlan1.90 to be configured.
P2(config-if)# ip address 46.1.1.1/24	Assign ip address
P2(config-if)# ip ospf cost 1	Change ospf cost of the link
P2(config-if)#interface vlan1.100	Specify interface vlan1.100 to be configured.
P2(config-if)# ip address 34.1.1.2/24	Assign ip address
P2(config-if)# ip ospf cost 1	Change ospf cost of the link
P2(config-if)#interface xe2	Enter interface mode
P2(config-if)# switchport	Set the interface as Layer2 port

`P2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)# switchport trunk allowed vlan add 70,79`	Enable VLAN's allowed on this interface.
`P2(config-if)# switchport trunk native vlan 79`	Configure native vlan
`P2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe3`	Enter interface mode
`P2(config-if)# switchport`	Set the interface as Layer2 port
`P2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)# switchport trunk allowed vlan add 90,99`	Enable VLAN's allowed on this interface.
`P2(config-if)# switchport trunk native vlan 99`	Configure native vlan
`P2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe7`	Enter interface mode
`P2(config-if)# switchport`	Set the interface as Layer2 port
`P2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)# switchport trunk allowed vlan add 30,39`	Enable VLAN's allowed on this interface.
`P2(config-if)# switchport trunk native vlan 39`	Configure native vlan
`P2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe9`	Enter interface mode
`P2(config-if)# switchport`	Set the interface as Layer2 port
`P2(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)# switchport trunk allowed vlan add 50,59`	Enable VLAN's allowed on this interface.
`P2(config-if)# switchport trunk native vlan 59`	Configure native vlan
`P2(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe10`	Enter interface mode

P2(config-if)# switchport	Set the interface as Layer2 port
P2(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P2(config-if)# switchport trunk allowed vlan add 50,59	Enable VLAN's allowed on this interface.
P2(config-if)# switchport trunk native vlan 59	Configure native vlan
P2(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
P2(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P2(config-if)#interface xe25	Enter interface mode
P2(config-if)# switchport	Set the interface as Layer2 port
P2(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P2(config-if)# switchport trunk allowed vlan add 100,109	Enable VLAN's allowed on this interface.
P2(config-if)# switchport trunk native vlan 109	Configure native vlan
P2(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
P2(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P2(config-if)#router ospf 1	Enter ospf configuration mode
P2(config-router)# ospf router-id 4.4.4.4	Configure ospf router id
P2(config-router)# bfd all-interfaces	Enable bfd in all ospf interfaces
P2(config-router)# network 4.4.4.4/32 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config-router)# network 14.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config-router)# network 24.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config-router)# network 34.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config-router)# network 45.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config-router)# network 46.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P2(config)#end	Exit config mode

P3

P3(config)#hostname P3	Configure hostname
P3(config)#bfd interval 3 minrx 3 multiplier 3	Configure bfd interval globally
P3(config)#qos enable	Enable qos

`P3(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE vlan bridge
`P3(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`P3(config)#no igmp snooping`	Disable igmp snooping messages globally
`P3(config)#vlan database`	Enter into the vlan database
`P3(config-vlan)# vlan 10-200 bridge 1 state enable`	Configure vlan 10-200 and associate with bridge 1
`P3(config-vlan)#interface lo`	Enter lo interface mode
`P3(config-if)# ip address 5.5.5.5/32 secondary`	Assign loopback ip
`P3(config-if)#interface vlan1.60`	Specify interface vlan1.60 to be configured.
`P3(config-if)# ip address 35.1.1.2/24`	Assign ip address
`P3(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P3(config-if)#interface vlan1.70`	Specify interface vlan1.70 to be configured.
`P3(config-if)# ip address 45.1.1.2/24`	Assign ip address
`P3(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P3(config-if)#interface vlan1.80`	Specify interface vlan1.80 to be configured.
`P3(config-if)# ip address 56.1.1.1/24`	Assign ip address
`P3(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P3(config-if)#interface vlan1.110`	Specify interface vlan1.1100 to be configured.
`P3(config-if)# ip address 15.1.1.2/24`	Assign ip address
`P3(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P3(config-if)#interface vlan1.160`	Specify interface vlan1.160 to be configured.
`P3(config-if)# ip address 25.1.1.2/24`	Assign ip address
`P3(config-if)# ip ospf cost 1`	Change ospf cost of the link
`P3(config-if)#interface xe2`	Enter interface mode
`P3(config-if)# switchport`	Set the interface as Layer2 port
`P3(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P3(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P3(config-if)# switchport trunk allowed vlan add 70,79`	Enable VLAN's allowed on this interface.
`P3(config-if)# switchport trunk native vlan 79`	Configure native vlan
`P3(config-if)# load-interval 30`	Configure load period in multiple of 30 seconds
`P3(config-if)# spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P3(config-if)#interface xe10`	Enter interface mode
`P3(config-if)# switchport`	Set the interface as Layer2 port
`P3(config-if)# bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P3(config-if)# switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.

P3(config-if)# switchport trunk allowed vlan add 60,69	Enable VLAN's allowed on this interface.
P3(config-if)# switchport trunk native vlan 69	Configure native vlan
P3(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
P3(config-if)# mtu 1600	Change interface mtu value
P3(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P3(config-if)#interface xe15	Enter interface mode
P3(config-if)# switchport	Set the interface as Layer2 port
P3(config-if)# bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P3(config-if)# switchport trunk allowed vlan add 80,89	Enable VLAN's allowed on this interface.
P3(config-if)# switchport trunk native vlan 89	Configure native vlan
P3(config-if)# load-interval 30	Configure load period in multiple of 30 seconds
P3(config-if)# mtu 1600	Change interface mtu value
P3(config-if)# spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P3(config-if)#router ospf 1	Enter ospf configuration mode
P3(config-router)# ospf router-id 5.5.5.5	Configure ospf router id
P3(config-router)# bfd all-interfaces	Enable bfd in all ospf interfaces
P3(config-router)# network 5.5.5.5/32 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)# network 15.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)# network 25.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)# network 35.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)# network 45.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)# network 56.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#end	Exit config mode

VTEP3:

VTEP3#configure terminal	
VTEP3(config)#hostname VTEP3	Enter configuration terminal
VTEP3(config)#mac vrf vrf1	Configure hostname
VTEP3(config-vrf)# rd 6.6.6.6:11	Configure mac vrf vrf1

`VTEP3(config-vrf)# route-target both 10.10.10.10:100`	Configure RD for vrf1
`VTEP3(config-vrf)#mac vrf vrf2`	Configure RT for vrf1
`VTEP3(config-vrf)# rd 6.6.6.6:12`	Configure mac vrf vrf2
`VTEP3(config-vrf)# route-target both 10.10.10.10:101`	Configure RD for vrf2
`VTEP3(config-vrf)# route-target both 10.10.10.10:102`	Configure RT for vrf2
`VTEP3(config-vrf)#bfd interval 3 minrx 3 multiplier 3`	Configure RT for vrf2
`VTEP3(config)#load-balance enable`	Configure bfd interval globally
`VTEP3(config)#load-balance ipv4 dest-ipv4 src-ipv4`	Enable load balancing
`VTEP3(config)#hardware-profile filter egress-ipv4 enable`	Enable load balnce based on souce and destination ip address
`VTEP3(config)#hardware-profile filter vxlan enable`	Enable hardware filter for egress ipv4
`VTEP3(config)#hardware-profile statistics ac-lif enable`	Enable vxlan in hardware
`VTEP3(config)#hardware-profile statistics tunnel-lif enable`	Enable statistics on vxlan access interface
`VTEP3(config)#nvo vxlan enable`	Enable statistics on vxlan tunnel interface
`VTEP3(config)#qos enable`	Enable vxlan
`VTEP3(config)#qos statistics`	Enable qos
`VTEP3(config)#bridge 1 protocol ieee vlan-bridge`	Enable qos statistics
`VTEP3(config)#no bridge 1 spanning-tree enable`	Configure IEEE vlan bridge
`VTEP3(config)#no igmp snooping`	Disable spanning tree in bridge 1 globally
`VTEP3(config)#vlan database`	Disable igmp snooping messages globally
`VTEP3(config-vlan)# vlan 10-200 bridge 1 state enable`	Enter into the vlan database
`VTEP3(config-vlan)#interface lo`	Configure vlan 10-200 and associate with bridge 1
`VTEP3(config-if)# ip address 6.6.6.6/32 secondary`	Enter lo interface mode
`VTEP3(config-if)#interface vlan1.80`	Assign loopback ip
`VTEP3(config-if)# ip address 56.1.1.2/24`	Specify interface vlan1.80 to be configured.
`VTEP3(config-if)# ip ospf cost 1`	Assign ip address
`VTEP3(config-if)#interface vlan1.90`	Change ospf cost of the link
`VTEP3(config-if)# ip address 46.1.1.2/24`	Specify interface vlan1.90 to be configured.
`VTEP3(config-if)# ip ospf cost 1`	Assign ip address
`VTEP3(config-if)#interface xe3`	Change ospf cost of the link
`VTEP3(config-if)# switchport`	Enter interface mode
`VTEP3(config-if)# bridge-group 1 spanning-tree disable`	Set the interface as Layer2 port

VTEP3(config-if)# switchport mode trunk	Associate the interface with bridge group 1 and disable spanning tree
VTEP3(config-if)# switchport trunk allowed vlan add 90,99	Set the switching characteristics of this interface to trunk mode.
VTEP3(config-if)# switchport trunk native vlan 99	Enable VLAN's allowed on this interface.
VTEP3(config-if)# load-interval 30	Configure native vlan
VTEP3(config-if)# spanning-tree edgeport	Configure load period in multiple of 30 seconds
VTEP3(config-if)#interface xe15	Set the port as an edge-port to enable rapid transitions
VTEP3(config-if)# bridge-group 1 spanning-tree disable	Enter interface mode
VTEP3(config-if)# switchport mode trunk	Associate the interface with bridge group 1 and disable spanning tree
VTEP3(config-if)# switchport trunk allowed vlan add 80,89	Set the switching characteristics of this interface to trunk mode.
VTEP3(config-if)# switchport trunk native vlan 89	Enable VLAN's allowed on this interface.
VTEP3(config-if)# load-interval 30	Configure native vlan
VTEP3(config-if)# mtu 1600	Configure load period in multiple of 30 seconds
VTEP3(config-if)# spanning-tree edgeport	Change interface mtu value
VTEP3(config-if)#interface xe33	Set the port as an edge-port to enable rapid transitions
VTEP3(config-if)# switchport	Enter interface mode
VTEP3(config-if)# bridge-group 1 spanning-tree disable	Set the interface as Layer2 port
VTEP3(config-if)# switchport mode trunk	Associate the interface with bridge group 1 and disable spanning tree
VTEP3(config-if)# switchport trunk allowed vlan add 120,125,165	Set the switching characteristics of this interface to trunk mode.
VTEP3(config-if)# switchport trunk native vlan 165	Enable VLAN's allowed on this interface.
VTEP3(config-if)# load-interval 30	Configure native vlan
VTEP3(config-if)# mtu 1600	Configure load period in multiple of 30 seconds
VTEP3(config-if)# spanning-tree edgeport	Change interface mtu value
VTEP3(config-if)#interface xe45	Set the port as an edge-port to enable rapid transitions
VTEP3(config-if)# switchport	Enter interface mode
VTEP3(config-if)# load-interval 30	Set the interface as Layer2 port
VTEP3(config-if)#interface xe46	Configure load period in multiple of 30 seconds
VTEP3(config-if)# switchport	Enter interface mode
VTEP3(config-if)# load-interval 30	Set the interface as Layer2 port
VTEP3(config-if)#router ospf 1	Configure load period in multiple of 30 seconds
VTEP3(config-router)# ospf router-id 6.6.6.6	Enter ospf configuration mode
VTEP3(config-router)# bfd all-interfaces	Configure ospf router id
VTEP3(config-router)# network 6.6.6.6/32 area 0.0.0.0	Enable bfd in all ospf interfaces

`VTEP3(config-router)# network 46.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)# network 56.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)#router bgp 100`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)# neighbor 1.1.1.1 remote-as 100`	Enter Router BGP mode and define the AS number 100.
`VTEP3(config-router)# neighbor 1.1.1.1 update-source lo`	Configure bgp remote-as 100 with neighbor IP
`VTEP3(config-router)# neighbor 2.2.2.2 remote-as 100`	Define BGP neighbors, to update the source routes with lo
`VTEP3(config-router)# neighbor 2.2.2.2 update-source lo`	Configure bgp remote-as 100 with neighbor IP
`VTEP3(config-router)# address-family l2vpn evpn`	Define BGP neighbors, to update the source routes with lo
`VTEP3(config-router-af)# neighbor 1.1.1.1 activate`	Enter in to bgp l2vpn evpn address-family
`VTEP3(config-router-af)# neighbor 2.2.2.2 activate`	Activate neigbors
`VTEP3(config-router-af)# exit-address-family`	Activate neigbors
`VTEP3(config-router)#nvo vxlan vtep-ip-global 6.6.6.6`	Exit from bgp l2vpn evpn address-family
`VTEP3(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Configure vxlan global ip
`VTEP3(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf1`	Create vnid 1
`VTEP3(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled`	Associate vnid with evpn and vrf1
`VTEP3(config-nvo)# vxlan host-reachability-protocol evpn-bgp vrf2`	Create vnid 1000
`VTEP3(config-nvo)#nvo vxlan access-if port-vlan xe45 3001`	Associate vnid with evpn and vrf2
`VTEP3(config-nvo-acc-if)# no shutdown`	Create vxlan access port port-vlan
`VTEP3(config-nvo-acc-if)# map vnid 1`	Unshut the access interface
`VTEP3(config-nvo-acc-if)#nvo vxlan access-if port xe46`	Map the vnid to access-if
`VTEP3(config-nvo-acc-if)# no shutdown`	Create vxlan access port
`VTEP3(config-nvo-acc-if)# map vnid 1000`	Unshut the access interface
`VTEP3(config-nvo-acc-if)#end`	Map the vnid to access-if

Validation

```
VTEP1#sh ip ospf neighbor

Total number of full neighbors: 3
```

```
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:30    12.1.1.2        vlan1.10              0
3.3.3.3           1   Full/DR         00:00:31    13.1.1.2        vlan1.20              0
4.4.4.4           1   Full/DR         00:00:33    14.1.1.2        vlan1.30              0


VTEP2#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:38    12.1.1.1        vlan1.10
0
3.3.3.3           1   Full/DR         00:00:39    23.1.1.2        vlan1.40              0
4.4.4.4           1   Full/DR         00:00:39    24.1.1.2        vlan1.50              0
P1#sh ip ospf neighbor

Total number of full neighbors: 4
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:39    13.1.1.1        vlan1.20
0
2.2.2.2           1   Full/Backup      00:00:38    23.1.1.1        vlan1.40
0
4.4.4.4           1   Full/DR         00:00:40    34.1.1.2        vlan1.100             0
5.5.5.5           1   Full/DR         00:00:36    35.1.1.2        vlan1.60              0

P2#sh ip ospf neighbor

Total number of full neighbors: 5
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:30    14.1.1.1        vlan1.30
0
2.2.2.2           1   Full/Backup      00:00:38    24.1.1.1        vlan1.50
0
3.3.3.3           1   Full/Backup      00:00:33    34.1.1.1        vlan1.100
0
5.5.5.5           1   Full/DR         00:00:30    45.1.1.2        vlan1.70              0
6.6.6.6           1   Full/DR         00:00:34    46.1.1.2        vlan1.90              0
P2#
P3#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
```

```
3.3.3.3          1   Full/Backup      00:00:34    35.1.1.1        vlan1.60
0
4.4.4.4          1   Full/Backup      00:00:34    45.1.1.1        vlan1.70
0
6.6.6.6          1   Full/DR          00:00:33    56.1.1.2        vlan1.80              0
P3#

VTEP3#sh ip bgp summary
BGP router identifier 6.6.6.6, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
1.1.1.1                 4   100   14        13      2     0     0  00:04:00
1
2.2.2.2                 4   100   17        15      2     0     0  00:05:10
0

Total number of neighbors 2
VTEP1#sh ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
2.2.2.2                 4   100   14        14      1     0     0  00:04:00
0
6.6.6.6                 4   100   13        14      1     0     0  00:04:00
0

Total number of neighbors 2

Total number of Established sessions 2
VTEP1#
VTEP2#sh ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
1.1.1.1                 4   100   14        14      2     0     0  00:04:00
1
6.6.6.6                 4   100   15        18      2     0     0  00:05:10
0

Total number of neighbors 2
```

```
Total number of Established sessions 2
VTEP2#
VTEP3#sh ip bgp summary
BGP router identifier 6.6.6.6, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
1.1.1.1                 4   100   14        13      2     0     0  00:04:00
1
2.2.2.2                 4   100   17        15      2     0     0  00:05:10
0

Total number of neighbors 2

Total number of Established sessions 2
VTEP3#
VTEP1#sh bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
2.2.2.2                 4   100   23        22      4     0     0  00:07:34
2      0      0      2      0      0
6.6.6.6                 4   100   21        22      4     0     0  00:07:34
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
VTEP1#
VTEP2#sh bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100   22        24      5     0     0  00:07:41
2      0      0      2      0      0
6.6.6.6                 4   100   24        27      5     0     0  00:08:51
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
```

```
VTEP2#
VTEP3#sh bgp l2vpn evpn summary
BGP router identifier 6.6.6.6, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100   23        21      5     0     0  00:07:44
2      0      0      2      0      0
2.2.2.2                 4   100   26        24      5     0     0  00:08:54
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
VTEP3#

VTEP1#show nvo vxlan mac-table
================================================================================
============================================================
                                                              VXLAN MAC Entries
================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                Status              AccessPortDesc
--------------------------------------------------------------------------------
------------------------------------------------------------

1         po1        1000   ----         0000.1111.1111 1.1.1.1
Static Local        -------             -------
1         po1        1000   ----         0000.1111.1112 1.1.1.1
Static Local        -------             -------
1         po1        1000   ----         0000.1111.1113 1.1.1.1
Static Local        -------             -------
1         po1        1000   ----         0000.1111.1114 1.1.1.1
Static Local        -------             -------
1         po1        1000   ----         0000.1111.1115 1.1.1.1
Static Local        -------             -------
1         po1        1000   ----         a82b.b57c.4470 1.1.1.1
Dynamic Local       -------             -------
1000      ----       ----   ----         a82b.b57c.4476 2.2.2.2
Dynamic Remote      -------             -------

Total number of entries are : 7

VTEP1#
VTEP2#sh nvo vxlan mac-table
================================================================================
============================================================
                                                              VXLAN MAC Entries
================================================================================
============================================================
```

```
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
-------------------------------------------------------------------------------
-------------------------------------------------------------

1         ----       ----   ----         0000.1111.1111 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1112 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1113 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1114 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1115 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         a82b.b57c.4470 1.1.1.1
Dynamic Remote       -------             -------
1000      po2        2000   ----         a82b.b57c.4476 2.2.2.2
Dynamic Local        -------             -------

Total number of entries are : 7

VTEP2#

VTEP3#sh nvo vxlan mac-table
===============================================================================
=============================================================
                                                          VXLAN MAC Entries
===============================================================================
=============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
-------------------------------------------------------------------------------
-------------------------------------------------------------

1         ----       ----   ----         0000.1111.1111 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1112 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1113 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1114 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1115 1.1.1.1
Static Remote        -------             -------
1         ----       ----   ----         a82b.b57c.4470 1.1.1.1
Dynamic Remote       -------             -------
1000      ----       ----   ----         a82b.b57c.4476 2.2.2.2
Dynamic Remote       -------             -------

Total number of entries are : 7

VTEP3#
VTEP1#show nvo vxlan access-if brief
```

```
                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe46       ---   ---   500000   1000      up      up
po1        1000  ---   500001   1         up      up

Total number of entries are 2
VTEP1#
VTEP2#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe47       ---   ---   500000   1         up      up
po2        2001  ---   500001   1000      up      up
po2        2000  ---   500002   1000      up      up

Total number of entries are 3
VTEP2#
VTEP3#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe45       3001  ---   500000   1         up      up
xe46       ---   ---   500001   1000      up      up

Total number of entries are 2
VTEP3#
VTEP1#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          6.6.6.6          Installed        00:03:59        00:03:59
1.1.1.1          2.2.2.2          Installed        00:03:59        00:03:59

Total number of entries are 2
VTEP1#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name     VNI-Type Type Interface ESI                             VLAN DF-Status
Src-Addr         Dst-Addr
-------------------------------------------------------------------------------
-----------------------------------------
1       ----         L2       NW   ----      ----                            ---- ----
1.1.1.1          6.6.6.6
```

```
1       ----        L2      NW   ----     ----                          ---- ----
1.1.1.1         2.2.2.2
1       ----        --      AC   po1      --- Single Hommed port ---    1000 ----
----            ----
1000    ----        L2      NW   ----     ----                          ---- ----
1.1.1.1         6.6.6.6
1000    ----        L2      NW   ----     ----                          ---- ----
1.1.1.1         2.2.2.2
1000    ----        --      AC   xe46     --- Single Homed Port ---     ---- ----
----            ----

Total number of entries are 10
VTEP1#
VTEP2#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed       00:03:59        00:03:59
2.2.2.2          6.6.6.6          Installed       00:05:09        00:05:09

Total number of entries are 2
VTEP2#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name    VNI-Type Type Interface ESI                           VLAN DF-Status
Src-Addr         Dst-Addr
--------------------------------------------------------------------------------
-----------------------------------------
1       ----        L2      NW   ----     ----                          ---- ----
2.2.2.2          1.1.1.1
1       ----        L2      NW   ----     ----                          ---- ----
2.2.2.2          6.6.6.6
1       ----        --      AC   xe47     --- Single Homed Port ---     ---- ----
----            ----
1000    ----        L2      NW   ----     ----                          ---- ----
2.2.2.2          1.1.1.1
1000    ----        L2      NW   ----     ----                          ---- ----
2.2.2.2          6.6.6.6
1000    ----        --      AC   po2      --- Single Hommed port ---    2001 ----
----            ----
1000    ----        --      AC   po2      --- Single Hommed port ---    2000 ----
----            ----

Total number of entries are 11
VTEP2#
VTEP3#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
6.6.6.6          1.1.1.1          Installed       00:03:58        00:03:58
```

```
6.6.6.6          2.2.2.2          Installed        00:05:08        00:04:03

Total number of entries are 2
VTEP3#sh nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________________
1        ----         L2       NW   ----      ----                         ---- ----
6.6.6.6          1.1.1.1
1        ----         L2       NW   ----      ----                         ---- ----
6.6.6.6          2.2.2.2
1        ----         --       AC   xe45      --- Single Hommed port ---    3001 ----
----             ----
1000     ----         L2       NW   ----      ----                         ---- ----
6.6.6.6          1.1.1.1
1000     ----         L2       NW   ----      ----                         ---- ----
6.6.6.6          2.2.2.2
1000     ----         --       AC   xe46      --- Single Homed Port ---     ---- ----
----             ----

Total number of entries are 10
VTEP3#
```

Virtual eXtensible Local Area Network Command Reference

Contents

This document contains these chapters and appendices:

CHAPTER 1 VXLAN Commands

This chapter describes the VXLAN commands:

- show bgp l2vpn evpn
- show bgp l2vpn evpn summary
- show nvo vxlan
- show nvo vxlan access-if-config
- show nvo vxlan arp-cache
- show nvo vxlan counters access-port
- show nvo vxlan counters network-port
- show nvo vxlan mac-table
- show nvo vxlan static host state
- show nvo vxlan tunnel
- show running-config nvo vxlan
- show evpn multi-homing all
- show evpn multihoming-status
- show nvo vxlan route-count
- show nvo vxlan vni-name
- shutdown
- vxlan host-reachability-protocol evpn-bgp

arp-cache disable

Use this command to disable the ARP cache for MAC/IP.

When the ARP cache is disabled on a VxLAN access port, OcNOS does not reply to any ARP arriving on this port from the cache. OcNOS withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ARP cache.

OcNOS also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then OcNOS advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also `nvo vxlan max-cache-disable`.

Use the `no` form of this command to enable ARP cache for MAC/IP.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax

```
arp-cache disable
no arp-cache disable
```

Parameters

None

Default

By default, the arp-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-cache disable
(config-nvo-acc-if)#exit
```

arp-nd flood-suppress

Use this command to completely restrict the flood of ARP/ND packets towards remote VTEPs or other access ports.

This command applies only when the ARP cache and ND cache are enabled. When the ARP cache is disabled, ARP flooding is not suppressed even if this command is given. When the ND cache is disabled, ND flooding is not disabled, even if this command is given.

Use the no form of this command to not restrict the flood of ARP/ND packets.

Command Syntax

```
arp-nd flood-suppress
no arp-nd flood-suppress
```

Parameters

None

Default

By default, the arp-nd flood-suppress option is disabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-nd flood-suppress
(config-nvo-acc-if)#exit
```

arp-nd refresh timer

Use this command to configure aging out the arp-cache and nd-cache entries for given time multiplied by 3 in seconds.

Use the no form of this command to remove the configuration.

Note: After this timer interval, it sends out ARP to revalidate and 3 times of this would lead to removal of the dynamic entry.

Command Syntax

```
nvo vxlan arp-nd refresh-timer <3-300000>
no nvo vxlan arp-nd refresh-timer
```

Parameters

<3-300000>	Refresh time in seconds

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#config mode
(config)#nvo vxlan arp-nd refresh-timer 100
(config)#no nvo vxlan arp-nd refresh-timer
```

clear mac address table dynamic vxlan

Use this command to clear dynamically learned MACs.

Command Syntax

```
clear mac address table dynamic vxlan
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear mac address table dynamic vxlan
```

clear nvo vxlan counters

Use this command to clear the counters of access ports or network ports.

Command Syntax

```
clear nvo vxlan counters((access-port (port IFNAME | port-vlan IFNAME VLAN_ID |
  all)) | (network-port (dst A.B.C.D | all)))
```

Parameters

`port`	Port
`IFNAME`	Interface name
`port-vlan`	VLAN port
`IFNAME`	Interface name
`VLAN_ID`	VLAN identifier
`A.B.C.D`	Tunnel destination IPv4 address
`all`	All access or network ports

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Example for clearing a VLAN port counter:

```
#clear nvo vxlan counters access-port port-vlan xe1 2
```

Example for clearing all access port counters:

```
#clear nvo vxlan counters access-port all
```

Example for clearing network port counters:

```
#clear nvo vxlan counters network-port dst 1.1.1.1
```

Example for clearing all network port counters:

```
#clear nvo vxlan counters network-port all
```

clear nvo vxlan mac-stale-entries

Use this command to clear MAC entries that are in discard state in the forwarding database.

Command Syntax

```
clear nvo vxlan mac-stale-entries (vnid <1-16777215> |)
```

Parameters

<1-16777215>	VXLAN network identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear nvo vxlan mac-stale-entries vnid 100
```

COS

Use this command to set a COS value and its direction.

Use the no form of this command to reset the COS value.

COS-DSCP mapping mode is configured globally.

Note: The COS value is not supported in configuring the access-port only.

Command Syntax

```
cos <0-7> (ingress|egress)
no cos <0-7> (ingress|egress)
```

Parameters

<0-7>	COS value
ingress	Ingress direction
egress	Egress direction

Default

By default, the COS priority is 0.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#cos 2 ingress
(config-nvo-acc-if)#cos 3 egress
(config)#exit
```

cos queue

Use this command to map a CoS to a queue.

Use the no form of this command to unmap a CoS from a queue.

Command Syntax

```
cos <0-7> queue <0-7>
no cos <0-7>
```

Parameters

<0-7>	COS value
<0-7>	Queue value

Default

By default, the COS priority is 0.

Command Mode

CoS queue profile mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#qos cos-queue-profile ingress 64
(config-cos-queue)#cos 2 queue 4
(config-cos-queue)#exit
```

description

Use this command to set a description for a port.

Use the no form of this command to remove the description for a port.

Command Syntax

```
description LINE
no description
```

Parameters

LINE	Maximum 32 characters describing this port.

Default

No default value is specified for description LINE commands.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#description member-port xe1 with vlan 2
(config-nvo-acc-if)#exit

#show running-config  nvo vxlan
!
nvo vxlan enable
!
nvo vxlan access-if port-vlan xe1 2
 description member-port xe1 with vlan 2
 no shutdown
```

dscp

Use this command to map an explicit DSCP value to an access-port.

Use the no form of this command to reset the DSCP value.

DSCP-DSCP mapping mode is configured globally.

Command Syntax

```
dscp <0-63> (ingress|egress)
no dscp <0-63> (ingress|egress)
```

Parameters

`<0-63>`	DSCP value
`ingress`	Ingress direction
`Egress`	Egress direction

Default

By default, the dscp priority is 0.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dscp 24 ingress
(config-nvo-acc-if)#dscp 32 egress
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port xe1
(config-nvo-acc-if)#dscp 24 ingress
(config-nvo-acc-if)#dscp 32 egress
(config-nvo-acc-if)#exit
```

dscp queue

Use this command to map a DSCP value to a queue.

Use the no form of this command to unmap a DSCP value from a queue.

Command Syntax

```
dscp <0-63> queue <0-7>
no dscp <0-63>
```

Parameters

<0-63>	DSCP value
<0-7>	Queue

Default

By default, the dscp priority is 0.

Command Mode

DSCP queue configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#qos dscp-queue-profile ingress 128
(config-dscp-queue)#dscp 24 queue 4
(config-dscp-queue)#exit
```

dynamic-learning disable

Use this command to disable dynamic learning of MACs at the access port.

This command also disables dynamic learning of MAC/IP from ARP/ND messages received on this access port.

Use the no form of this command to enable dynamic learning of MACs at the access port.

Command Syntax

```
dynamic-learning disable
no dynamic-learning disable
```

Parameters

None

Default

By default, the dynamic-learning option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dynamic-learning disable
(config-nvo-acc-if)#exit
```

encapsulation

Use this command to assign a Tag Protocol Identifier (TPID) to an access port.

Use the no form of this command to set the default TPID (0x8100: IEEE 802.1Q VLAN-tagged frame) to an access port.

Command Syntax

```
dynamic-learning disable
no dynamic-learning disable
```

Parameters

TPID	Tag Protocol Identifier:
	Ox88A8: IEEE 802.1ad Provider Bridging
	Ox9100: IEEE 802.1Q VLAN-tagged frame with double tagging

Default

The encapsulation TPID default is 0X8100.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dynamic-learning disable
(config-nvo-acc-if)#exit
```

evpn esi hold-time

Use this command to allow some time for the tunnels to come at the time of VxLAN initialization before making the ESI up. This avoids traffic to be black-holed when a new PE is added and connected to an already running CE for multihoming.

Use the no form of this command to make the ESI up immediately when configuring the access-if cli.

Command Syntax

```
evpn esi hold-time <10-300>
no evpn esi hold-time <10-300>
```

Parameters

<10-300>	Hold time in seconds

Default

The default value is 0.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# evpn esi hold-time 100
(config)# exit
```

evpn multi-homed

Use this command to configure interfaces as multi-homed and configure esi-value for physical and static LAGs, and system-mac for dynamic LAGs.

Use the no parameter of this command to unconfigure multi-homing on an interface.

Command Syntax

```
evpn multi-homed (esi XX:XX:XX:XX:XX:XX:XX:XX:XX | system-mac (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
no evpn multi-homed (esi | system-mac)
```

Parameters

`XX:XX:XX:XX:XX:XX:XX:XX:XX`

ESI value in HH:HH:HH:HH:HH:HH:HH:HH:HH - 9 octet format

`XX-XX-XX-XX-XX-XX`

Host MAC address (Option 1)

`XX:XX:XX:XX:XX:XX`

Host MAC address (Option 2)

`XXXX.XXXX.XXXX`

Host MAC address (Option 3)

Default

The default value is 0.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config)#evpn multi-homed esi 00:11:22:33:44:55:66:77:88
(config)#exit

configure terminal
(config)#interface po1
(config)#evpn multi-homed system-mac 0000.0000.1111
(config)#exit
```

evpn vxlan multihoming enable

Use this command to enable evpn vxlan multi-homing

Use the no form of this command to disable evpn vxlan multi-homing.

Note: You must restart the device after giving this command. If there are devices in the topology which have multi-homed CEs, then devices which do not have multi-homed CEs should also enable multihoming so that they can load share traffic to the multi-homed CEs.

Note: Before enabling multi-homing, configure the hardware-profiles:

- hardware-profile filter vxlan-mh
- hardware-profile filter with the `egress-ipv4` parameter

Command Syntax

```
evpn vxlan multihoming enable
no evpn vxlan multihoming enable
```

Parameters

None

Default

By default, multi-homing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS-SP version 4.0.

Example

```
#configure terminal
#(config)#evpn vxlan multihoming enable
#(config)#exit
```

hardware-profile filter vxlan

Use this command to configure hardware profile for nvo vxlan. This profile should be enabled before enabling VXLAN.

Note: You need to save the configuration and do a reboot after giving this command.

Command Syntax

```
hardware-profile filter vxlan enable
hardware-profile filter vxlan disable
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#config mode
(config)# hardware-profile filter vxlan enable
(config)# hardware-profile filter vxlan disable
```

hardware-profile filter vxlan-mh

Use this command to enable the hardware-profile for VXLAN multi-homing to successfully activate multi-homing in the hardware.

Before enabling EVPN multi-homing (evpn multi-homed command), give this command.

Before disabling the hardware-profile, disable EVPN multi-homing.

Note: You need to save the configuration and do a reboot after giving this command.

Use the `disable` form of this command to disable the configured hardware-profile.

Command Syntax

```
hardware-profile filter vxlan-mh enable
hardware-profile filter vxlan-mh disable
```

Parameters

None

Default

By default, the VXLAN multi-homing hardware-profile is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
#(config)#hardware-profile filter vxlan-mh enable
#(config)#hardware-profile filter vxlan-mh disable
#(config)#exit
```

mac

Use this command to associate a static MAC address and a static IPv4 address on an access interface.

Use the no form of this command to disassociate a static MAC address and an IPv4 address for an access interface.

Note: When a static host is configured on an access port which is in the down state, its state is Inactive.

Note: The same static mac configuration is not allowed on a different access port as then there will be a chance of conflict. However, if a dynamic packet is sent at another access port which is up and running with the same MAC, it learns as usual. As soon as the port on which the static MAC is configured comes up, static learning is given precedence and the dynamically learned MAC is moved to the port where it is configured statically.

Command Syntax

```
mac XXXX.XXXX.XXXX (| ip A.B.C.D)
no mac XXXX.XXXX.XXXX (| ip A.B.C.D)
```

Parameters

XXXX.XXXX.XXXX	Static MAC address. The following formats are supported:
	XX-XX-XX-XX-XX-XX Source MAC address (Option 1)
	XX:XX:XX:XX:XX:XX Source MAC address (Option 2)
	XXXX.XXXX.XXXX Source MAC address (Option 3)
A.B.C.D	Static IPv4 address.

Default

No default value is specified for mac command.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#mac 0000.0000.aaaa ip 10.10.10.1
(config-nvo-acc-if)#mac 0000.0000.aaa1
(config-nvo-acc-if)#exit
```

mac vrf

Use this command to create a MAC VRF to use in EVPN routes.

Limitation: If the VRF is linked with a VxLAN identifier, then it cannot be deleted and any route distinguisher or route target configured on it cannot be changed.

See also vxlan host-reachability-protocol evpn-bgp.

Use the no form of this command to delete the MAC VRF.

Command Syntax

```
mac vrf WORD
no mac vrf WORD
```

Parameter

WORD	MAC routing or forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mac vrf vrf1

(config)#no mac vrf vrf1
```

mac-holdtime

Use this command to set the MAC hold time for a MAC/IP or MAC.

The feature holds the MAC in hardware until BGP has withdrawn from the neighbors. This helps to reduce flooding to other access ports.

This setting applies when the access port is shut down, the physical port on which the access port is down, or the access port is removed from the VNID using the no form of the map vnid command.

When the MAC hold time is configured as -1, then the MAC is not removed from the hardware and is also not withdrawn from EVPN BGP.

Use the no form of this command to remove the MAC hold time for the MAC/IP or MAC.

Note: When a MAC is moved to discard state, traffic to and from this MAC is discarded. This is applicable only on statically configured MAC/MAC-IPs.

Command Syntax

```
mac-holdtime <-1-300>
no mac-holdtime
```

Parameter

<-1-300>	MAC hold time in seconds. Specify -1 to "never expire".

Default

The default holdtime for mac is 3 seconds.

Command Mode

NVO mode and NVO_ACC_IF_MODE mode

Note: When configured in both modes, then the NVO_ACC_IF_MODE value takes preference for that access port.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan id 3 ingress-replication inner-vid-disabled
(config-nvo)#mac-holdtime -1
(config-nvo)#exit
```

map qos-profile

Use this command to map a QoS profile created with `qos cos-queue-profile` or `qos dscp-queue-profile` to an access port.

Use the no form of this command to unmap a QoS profile from an access port.

Command Syntax

```
map qos-profile (ingress|egress) <1-128>
no map qos-profile (ingress|egress)
```

Parameters

`ingress`	Ingress direction (access network)
`egress`	Egress direction (network access)
`<1-128>`	QoS profile identifier

Default

No default value is specified for map qos-profile command.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#map qos-profile ingress 64
(config-nvo-acc-if)#map qos-profile egress 100
(config-nvo-acc-if)#exit
```

map vnid

Use this command to map a tenant to an access-port.

Use the no form of this command to remove the tenant from an access-port.

See also nvo vxlan id.

Command Syntax

```
map vnid <1-16777215>
no map vnid <1-16777215>
```

Parameters

<1-16777215>	VxLAN network identifier

Default

No default value is specified for map vnid command.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#map vnid 100
(config-nvo-acc-if)#exit
```

nd-cache disable

Use this command to disable ND cache for MAC/IPv6.

When the ND cache is disabled on a VxLAN access port, OcNOS does not reply to any ND arriving on this port from the cache. OcNOS withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ND cache.

OcNOS also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then OcNOS advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also `arp-cache disable`.

Use the `no` form of this command to enable ND cache for MAC/IPv6.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax

```
nd-cache disable
```

```
no nd-cache disable
```

Parameters

None

Default

By default, the nd-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#nd-cache disable
(config-nvo-acc-if)#exit
```

nvo vxlan

Use this command to enable or disable VxLAN.

You must enable the VXLAN hardware profile with the hardware-profile filter vxlan command before enabling VxLAN.

Command Syntax

```
nvo vxlan (enable | disable)
```

Parameters

None

Default

By default, the VxLAN is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan enable

(config)#nvo vxlan disable
```

nvo vxlan access-if

Use this command to map a complete interface or a VLAN on an interface to identify the tenant traffic and to enter NVO access interface mode.

Use the no form of this command to unmap an interface or a VLAN.

Note: When a VxLAN access interface configured as a port VLAN is unconfigured, the traffic sent on the VLAN for that port hits some QoS policies which are set to not accept VLAN traffic on a port for which the VLAN is not configured. Such traffic is counted as VxLAN/ACL discards.

Command Syntax

```
nvo vxlan access-if (port IFNAME | port-vlan IFNAME VLAN_ID)
no nvo vxlan access-if (port IFNAME | port-vlan IFNAME VLAN_ID)
```

Parameters

port	A physical port.
IFNAME	Interface name (Physical/Static lag/Dynamic lag)
port-vlan	The physical port on which VLANs are configured
IFNAME	Interface name (Physical/Static lag/Dynamic lag)
VLAN_ID	VLAN identifier.

Default

By default, the nvo vxlan access-if option is port VLAN ID.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port xe1
(config-nvo-acc-if)#exit
```

nvo vxlan id

Use this command to add a tenant and the type of VPN. This command changes the mode to NVO mode.

Use no form of this command to unconfigure the VXLAN ID.

You must enable VXLAN with the nvo vxlan command before you give this command.

Command Syntax

```
nvo vxlan id <1-16777215> (multicast |) | (ingress-replication (| inner-vid-
  disabled)))
no nvo vxlan id <1-16777215> (multicast |) | (ingress-replication (| inner-vid-
  disabled)))
```

Parameters

`<1-16777215>`	VxLAN Network Identifier (VNID)
`multicast`	Point to multipoint.
`ingress-replication`	Use head end replication for forwarding BUM (Broadcast, Unknown Unicast, Multicast) traffic
`inner-vid-disabled`	Do not carry VID out of network port

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan id 300 ingress-replication
(config-nvo)#exit

(config)#nvo vxlan id 200 ingress-replication inner-vid-disabled
(config-nvo)#exit
```

nvo vxlan mac-ageing-time

Use this command to set the dynamically learned MAC aging time.

Use the no form of this command to set the age out the MACs in hardware to its default (300 seconds).

Command Syntax

```
nvo vxlan mac-ageing-time <10-1000000>
no nvo vxlan mac-ageing-time
```

Parameters

<10-1000000>	Aging time in seconds

Default

The default age out time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan mac-ageing-time 10
```

nvo vxlan max-cache-disable

Use this command to configure the maximum number of ARP and ND cache disables on access ports configured with the port+VLAN options. This command does not limit the ARP and ND cache disables on access ports created with only the port option.

Use the no form of this command to set the maximum number of ARP and ND cache disables to its default (0).

Note: If any mac is in conflict when the max cache disable is being unconfigured, then the corresponding caches will not be enabled. This can be enabled after manually, removing the conflict. Caches where there is no conflict, are enabled.

Command Syntax

```
nvo vxlan max-cache-disable <1-200>
no nvo vxlan max-cache-disable
```

Parameters

<-1-200>	Number of ARP/ND cache disable allowed

Default

The default maximum number of ARP and ND cache disables is 0.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#nvo vxlan max-cache-disable 10
(config-nvo)#exit
```

nvo vxlan tunnel qos-map-mode

Use this command to configure QoS COS-DSCP or DSCP-DSCP mapping for a tunnel in the ingress or egress direction.

Use the no form of this command to remove QoS mapping for a tunnel.

Command Syntax

```
nvo vxlan tunnel qos-map-mode (cos-dscp|dscp-dscp) (ingress|egress) (<65-128>|)
nvo vxlan tunnel qos-map-mode (cos-dscp|dscp-dscp) (ingress|egress)
```

Parameters

`cos-dscp`	COS-to-DSCP mapping: the COS in packets entering on an access port is copied to the DSCP field of VXLAN header in packets exiting the tunnel
`dscp-dscp`	DSCP-to-DSCP mapping: the DSCP in packets entering on an access port is copied to the DSCP field of VXLAN header in packets exiting the tunnel
`ingress`	Ingress direction (access network)
`egress`	Egress direction (network access)
`<65-128>`	QoS profile ID

Default

No default value is specified for nvo vxlan tunnel qos-map-mode command.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress
(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress 128
(config)#exit

#configure terminal
(config)#nvo vxlan tunnel qos-map-mode dscp-dscp ingress
(config)#nvo vxlan tunnel qos-map-mode dscp-dscp egress 128
(config)#exit
```

nvo vxlan vtep-ip-global

Use this command to set the source IP address of the VxLAN tunnels.

Use the no form of this command to remove the source IP address of the VxLAN tunnels.

You must enable VXLAN with the nvo vxlan command before you give this command.

Command Syntax

```
nvo vxlan vtep-ip-global A.B.C.D
no nvo vxlan vtep-ip-global A.B.C.D
```

Parameters

A.B.C.D	Source VTEP IP address of the global configuration

Default

No default value is specified for nvo vxlan vtep-ip-global command.

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config-nvo)#nvo vxlan vtep-ip-global 10.10.11.1
```

qos cos-queue-profile

Use this command to create a QoS COS queue profile and enter COS queue profile mode.

Use the no form of this command to remove a COS queue profile.

Command Syntax

```
qos cos-queue-profile (ingress|egress) <1-64>
no qos cos-queue-profile <1-64>
```

Parameters

ingress	Ingress direction (access network)
egress	Egress direction (network access)
<1-128>	QoS profile identifier

Default

No default value is specified for qos cos-queue-profile command.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#qos cos-queue-profile ingress 64
(config-cos-queue)#exit
```

qos dscp-queue-profile

Use this command to configure create a QoS DSCP queue profile and enter DSCP queue profile mode.

Use the no form of this command to remove a QoS DSCP queue profile.

Command Syntax

```
qos dscp-queue-profile (ingress|egress) <65-128>
no qos dscp-queue-profile <65-128>
```

Parameters

ingress	Egress direction
egress	Ingress direction
<1-128>	QoS profile identifier

Default

No default value is specified for qos dscp-queue-profile command.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#qos dscp-queue-profile ingress 128
(config-dscp-queue)#exit
```

show bgp l2vpn evpn

Use this command to display details about Layer 2 Virtual Private Network (L2VPN) Ethernet Virtual Private Network (EVPN) routes.

Note: A BGP EVPN route update received for an unreachable IP address is also listed by this command and as a best route. This is because the next hop tracking feature is not supported for the EVPN address family. However, the tunnel to this IP address is shown in unresolved state by the show nvo vxlan tunnel output.

Command Syntax

```
show bgp l2vpn evpn ((vrf WORD)|(rd WORD)| time|)
show bgp l2vpn evpn mac-ip ((vrf WORD)|(rd WORD)|)
show bgp l2vpn evpn mcast
show bgp l2vpn evpn multihoming es-route <(rd WORD)|(vrf WORD)>
show bgp l2vpn evpn multihoming ethernet-ad-per-evi <(rd WORD)|(vrf WORD)>
show bgp l2vpn evpn multihoming ethernet-ad-per-es <(rd WORD)|(vrf WORD)>
```

Parameters

`vrf`	Virtual Routing and Forwarding instance
`WORD`	VRF name
`rd`	Route distinguisher
`WORD`	Route distinguisher: ASN:nn or IP:nn
`time`	Display learned time for EVPN routes
`mac-ip`	MAC/IP routes (EVPN type 2)
`mcast`	Multicast routes (EVPN type 3)

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp l2vpn evpn

BGP table version is 25, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
```

```
    Network          Next Hop            Metric     LocPrf       Weight Path  Peer

RD[1.1.1.1:1] VRF[vrfblue]:
*>   [2]:[0]:[100]:[48,0000:00aa:aaaa]:[32,10.1.1.2]:[100]
                      1.1.1.1             0          100            32768    i
*>i  [2]:[0]:[100]:[48,0000:00bb:bbbb]:[32,10.1.1.3]:[100]
                      4.4.4.4             0          100            0        i  10.1.1.1
*>   [3]:[100]:[32,1.1.1.1]
                      1.1.1.1             0          100            32768    i
*>i  [3]:[100]:[32,4.4.4.4]
                      4.4.4.4             0          100            0        i  10.1.1.1
*>   [3]:[101]:[32,1.1.1.1]
                      1.1.1.1             0          100            32768    i
*>i  [3]:[101]:[32,4.4.4.4]
                      4.4.4.4             0          100            0        i  10.1.1.1

RD[2.2.2.2:1]
*>i  [2]:[0]:[100]:[48,0000:00bb:bbbb]:[32,10.1.1.3]:[100]
                     4.4.4.4              0          100            0        i  10.1.1.1
*>i  [3]:[100]:[32,4.4.4.4]
                      4.4.4.4             0          100            0        i  10.1.1.1
*>i  [3]:[101]:[32,4.4.4.4]
                      4.4.4.4             0          100            0        i  10.1.1.1

Total number of prefixes 9
```

Table 1-84 shows the status codes displayed at the start of a route entry.

Table 1-84: status codes

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.
l	labeled	BGP Labeled Unicast advertises route information between inter region routers.

Table 1-85 shows the codes at the end of each route entry that indicate where the route originated.

Table 1-85: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 1-86 explains the fields for each route.

Table 1-86: route entry fields

Field	Description
RD	Route distinguisher: AS number or IP address.
VRF	Name of the VRF.
Network	EVPN route information. The route type indicates the type of routing information advertised by the EVPN control plane: 2 MAC/IP Route: Endpoint reachability information, including MAC and IP addresses of the endpoints. 3 Inclusive Multicast Route: Information about how to forward Broadcast, Unknown Unicast and Multicast (BUM) traffic. The other fields included depend on the route type: Type 2: [ESI]:[E-Tag]:[Length, Host MAC address]:[Length, Host IP address]:[Label/VNID] Type 3: [E-Tag]:[Length, PE IP address] ESI (Ethernet Segment Identifier): a unique non-zero identifier that identifies an Ethernet segment, which is a set of links that connects a network or device to one or more PEs. ESI 0 denotes a single-homed site. E-Tag (Ethernet tag): identifies a particular broadcast domain such as a VLAN or VNID in the VxLAN case. An EVPN instance consists of one or more broadcast domains. VNID (VXLAN network identifier): identifies Layer 2 segments and maintains Layer 2 isolation between the segments, allowing the addressing of up to 16 million logical networks in the same administrative domain. The status codes are explained in Table 1-84.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.
LocPrf	This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

Table 1-86: route entry fields (Continued)

Field	Description
Path	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 1-85.
Peer	Neighbor address.
Total number of prefixes	The total number of prefixes listed.

show bgp l2vpn evpn summary

Use this command to display a summary of BGP EVPN neighbor status.

Command Syntax

```
show bgp l2vpn evpn summary
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 17
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd     AD  MACIP  MCAST    ESI
8.8.8.8                 4   100  111        112      17      0      0  00:53:03              3      0      0      3      0
9.9.9.9                 4   100  110        110      17      0      0  00:52:10             15      0     13      2      0
13.13.13.13             4   100  132        109      17      0      0  00:51:57              4      0      2      2      0

Total number of neighbors 3

Total number of Established sessions 3
```

The start of the output shows:

- The BGP router identifier and the local router AS number.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- BGP AS-PATH entry and community entries.

Table 1-87 explains the fields for each neighbor entry.

Table 1-87: neighbor fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.
MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.

Table 1-87: neighbor fields (Continued)

Field	Description
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.
OutQ	Messages waiting in the output queue to be sent.
Up/Down	Connection up time in the interface.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keep alive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keep alive messages with its peer Invalid: The session state is invalid.
AD	Number of EVPN type 1 Ethernet Auto-discovery routes: Only originated for multi-homed sites. Type 1 routes allow fast convergence where PE devices can change the next-hop adjacencies for all MAC addresses associated with a particular Ethernet Segment and aliasing where traffic can be balanced across multiple egress points
MACIP	Number of EVPN type 2 MAC/IP routes: Endpoint reachability information, including MAC and IP addresses of the endpoints.
MCAST	Number of EVPN type 3 Inclusive Multicast routes: Broadcast, Unknown Unicast and Multicast (BUM) traffic.
ESI	Number of EVPN type 4 Ethernet Segment Routes: Used in multi-homing for Designated Forwarder Election. The Designated Forwarder sends BUM traffic to the CE on a particular Ethernet Segment.

show nvo vxlan

Use this command to display VXLAN information.

Command Syntax

```
show nvo vxlan (vnid <1-16777215>|)
```

Parameters

<1-16777215>	VXLAN network identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     Vni-name     Type Interface ESI                             Vlan DF-Status Src-addr         Dst-addr
------------------------------------------------------------------------------------------------------------
10       ----         NW   ----      ----                            ---- ----      1.1.1.1          3.3.3.3
10       ----         NW   ----      ----                            ---- ----      1.1.1.1          2.2.2.2
10       ----         AC   ce21/1    00:00:11:22:33:44:55:66:77:88 2    DF        ----             ----
20       ----         NW   ----      ----                            ---- ----      1.1.1.1          3.3.3.3
20       ----         NW   ----      ----                            ---- ----      1.1.1.1          2.2.2.2
20       ----         AC   ce21/1    00:00:11:22:33:44:55:66:77:88 3    NON-DF    ----             ----

Total number of entries are 6
```

Table 1-88 explains the fields in the output.

Table 1-88: VxLAN fields

Field	Description
VNID	VXLAN network identifier.
Type	NW - Network Port: VxLAN tunnel AC - Access Port: Host connection
Interface	Name of the Interface.
Vlan	VLAN identifier
Src-addr	Source address in the interface.
Dst-addr	Destination address in the interface.
Total number of entries	The total number of entries listed.

show nvo vxlan access-if-config

Use this command to display the current running configuration of the access interface.

Command Syntax

```
show nvo vxlan access-if-config (LINE|)
```

Parameters

LINE	Access port description

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan access-if-config
     nvo vxlan access-if port-vlan xe1 2
      map vnid 100
access-if-description member-port with xe1 as vlan 2
shutdown
mac 0000.0000.1111
mac 0000.0000.aaaa  ip 12.12.12.1
map qos-profile cos-to-queue ac_port_ingress
     !
     nvo vxlan access-if port-vlan po1 6
      no shutdown
      map vnid 100
     !
```

show nvo vxlan arp-cache

Use this command to display the ARP cache information.

Command Syntax

```
show nvo vxlan arp-cache (vnid <1-16777215>|)
```

Parameters

<1-16777215>	VXLAN network identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan  arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       12.12.12.2       0000.0000.2222 Static Local   ----
Total number of entries are 1
```

Table 1-89 explains the fields in the output.

Table 1-89: arp cache fields

Field	Description
VNID	VXLAN network identifier.
Ip-Addr	IP address of the vxlan.
Mac-Addr	Device MAC address.
Type	How a host learns a MAC/IP pair: Dynamic Local: Learned by data plane source learning Dynamic Remote: Learned by EVPN Type 2 (MAC/IP) routes Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP
Total number of entries	The total number of entries listed.

show nvo vxlan counters access-port

Use this command to display the receive and transmit counters of an access port.

Note: Due to a limitation in the hardware, the transmit packet counters includes the BUM traffic received on that port.

Note: To see the statistics, you must enable the hardware profile for the access-port with the hardware-profile filter command with the `ac-lif` parameter.

Note: All the expected packets might not be seen in the output of this command.

Command Syntax

```
show nvo vxlan counters access-port (port IFNAME | port-vlan IFNAME VLAN_ID | all)
```

Parameters

`IFNAME`	Access port name
`VLAN_ID`	VLAN identifier
`all`	All ports and VLANs

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan  counters access-port port-vlan xe13 10

Data packets:
   *If ARP/ND cache is enabled, TX doesn't count ARP/ND replies
 from  ARP/ND cache and ARP/ND forwarded after uplifting to
 the control plane.
   RX:  packets  : 2774939
        bytes    : 210553516
   TX:  packets  : 4322274
        bytes    : 326026474

Control Packets:
 *ARP/ND uplifted and sent/replied from control plane:
  Rx Vxlan Arp discard count           : 0
  Rx Vxlan Nd discard count            : 0
  Tx Vxlan Arp discard count           : 0
  Tx Vxlan Nd discard count            : 0
  Rx Vxlan Arp Request count           : 0
  Tx Vxlan Arp Request count           : 0
  Rx Vxlan Arp Reply count             : 5
  Tx Vxlan Arp Reply count             : 1
  Rx Vxlan Neighbor Solicitation count : 0
  Tx Vxlan Neighbor Solicitation count : 0
  Rx Vxlan Neighbor Advertisement count: 3
  Tx Vxlan Neighbor Advertisement count: 0
```

Table 1-90 explains the fields in the output.

Table 1-90: access port counters

Field	Description
RX: packets	Number of packets received on an access-interface.
RX: bytes	Number of bytes received.
TX: packets	Number of packets transmitted.
TX: bytes	Number of bytes transmitted.
Rx Vxlan Nd discard count	Number of discarded ND that is received from neighbor.
Tx Vxlan Arp discard count	Number of discarded Arp that is transmitted to peer.
Tx Vxlan Nd discard count	Number of discarded ND that is transmitted to peer.
Rx Vxlan Arp Request count	Number of request ARP that is received from neighbor.
Tx Vxlan Arp Request count	Number of request ARP that is transmitted to peer.
Rx Vxlan Arp Reply count	Number of replied ARP that is received from neighbor.
Tx Vxlan Arp Reply count	Number of replied ARP which is transmitted to peer.
Rx Vxlan Neighbor Solicitation count	Number of request ND that is received from neighbor.
Tx Vxlan Neighbor Solicitation count	Number of replied ND that is received from neighbor.
Rx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement that is received from neighbor.
Tx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement which is transmitted to peer.

show nvo vxlan counters network-port

Use this command to display the receive and transmit counters of a network port including ARP, ND and GARP counters.

Command Syntax

```
show nvo vxlan counters network-port (dst A.B.C.D | ALL)
```

Parameters

A.B.C.D	Tunnel IPv4 address
ALL	All addresses

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan counters network-port dst 2.2.2.2

Data packets:
  *If ARP/ND cache is enabled, TX doesn't count ARP/ND replies
from  ARP/ND cache and ARP/ND forwarded after uplifting to
the control plane.
  RX:  packets  : 0
       bytes    : 0
  TX:  packets  : 3570006
       bytes    : 406980684

Control Packets:
*ARP/ND uplifted and sent/replied from control plane:
 TX VXLAN ARP discard count           : 0
 TX VXLAN ND discard count            : 0
 Tx Vxlan ARP Request count           : 0
 Tx Vxlan ARP Reply count             : 0
 Tx Vxlan Neighbor Solicitation count : 0
 Tx Vxlan Neighbor Advertisement count: 0
```

Table 1-91 explains the each network entry fields.

Table 1-91: show nvo vxlan counters network-port output fields

Field	Description
RX: packets	Number of hello packets received from neighbor.
RX: bytes	Number of hello packets received from neighbor in bytes received.

Table 1-91: show nvo vxlan counters network-port output fields (Continued)

Field	Description
TX: packets	Number of hello packets transmitted to neighbor.
TX: bytes	Number of hello packets transmitted to neighbor in bytes transmitted.
Tx Vxlan Arp discard count	Number of discarded Arp that is transmitted to peer.
Tx Vxlan Nd discard count	Number of discarded ND that is transmitted to peer.
Tx Vxlan Arp Request count	Number of request ARP that is transmitted to peer.
Tx Vxlan Arp Reply count	Number of replied ARP which is transmitted to peer.
Tx Vxlan Neighbor Solicitation count	Number of replied ND that is received from neighbor.
Tx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement which is transmitted to peer.

show nvo vxlan mac-table

Use this command to display the host MAC address table. Use the hardware option to see the ageout time for the dynamically learn macs.

Command Syntax

```
show nvo vxlan mac-table (vnid <1-16777215>|) (summary | hardware|)
```

Parameters

<1-16777215>	VXLAN network identifier
summary	Display a count of MAC addresses
hardware	Display hardware information

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan mac-table
================================================================================================
============================================================
                      VXLAN MAC Entries
================================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
____________________________________________________________


10        ce21/1     2      ----         0000.0000.1111 1.1.1.1
Static Local         -------             partner-port
10        ----       ----   ----         0000.0000.2222 3.3.3.3
Static Remote        -------             -------
20        ce21/1     3      ----         0000.0000.cccc 1.1.1.1
Static Local         Discard             -------
20        ----       ----   ----         0000.0000.dddd 3.3.3.3
Static Remote        -------             -------

Total number of entries are : 4

#show nvo vxlan mac-table hardware
================================================================================================
============================================================
                         VXLAN MAC Entries
================================================================================================
============================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            Time-out AccessPortDesc
```

```
10          ce21/1    2       ---          0000.0000.1111 1.1.1.1
Static Local          -----               ---      partner-port
10          ---       ---     ---          0000.0000.2222 3.3.3.3
Dyanamic Remote       -----               ---
10          ---       ---     ---          0000.0000.aa11 3.3.3.3
Dyanamic Remote       -----               ---
10          ce21/1    2       ---          0000.0000.bb11 1.1.1.1
Dynamic Local         -----               300      partner-port
10          ce21/1    2       ---          0000.0000.bb12 1.1.1.1
Dynamic Local         -----               277      partner-port
20          ce21/1    ---     ---          0000.0000.cccc 1.1.1.1
Static Local          Discard             ---
20          ---       ---     ---          0000.0000.dddd 3.3.3.3
Dyanamic Remote       -----               ---

Total number of entries are 7
```

Table 1-92 explains the fields in the output.

Table 1-92: MAC table fields

Field	Description
VNID	VXLAN network identifier
Interface	Interface name
VlanId	VLAN identifier
Mac-Addr	MAC address
VTEP-Ip	VTEP identifier
Type	How a host learns a MAC/IP pair: Dynamic Remote: Learned by EVPN Type 2 (MAC/IP) routes Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP Dynamic Local: Learned by data plane source learning
Status	Max Move conflict: When a MAC has moved too many times (5 or more times in 180 seconds). This is according to the procedures defined in RFC 7432, Section 15.1. Discard: If a MAC hold time is configured, then if the VxLAN access port goes down (admin or operational), the MAC is moved to the discard state for the period of the hold time. The MAC is also moved to the discard state if the VNID is unmapped from the port. In dynamically learned cases, the MAC is also moved to discard when learning is disabled.
Time-out	Age timeout for dynamically learned MACs.
AccessPortDesc	Access port description.
Total number of entries	The total number of entries listed.

show nvo vxlan static host state

Use this command to display the state of the host which is configured statically.

Command Syntax

```
show nvo vxlan static host state
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan  static host state
VXLAN Static Host Information
=============================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     Ifname       Outer-Vlan Inner-vlan Ip-Addr                                  Mac-
Addr       Status
_____________________
10       xe13         10         ---        12.12.12.2
0000.0000.2222 Active
10       xe17         10         ---        11.11.11.1
0000.0000.bbbb Inactive
10       xe17         30         40         0.0.0.0
0000.1111.2222 Inactive

Total number of entries are 5
```

Table 1-93 explains the output fields.

Table 1-93: Static host fields

Field	Description
VNID	VXLAN network identifier
Ifname	Interface name
Vlan	VLAN name
Ip-Addr	IP address

Table 1-93: Static host fields

Field	Description
Mac-Addr	MAC address
Status	Status of the MAC/IP on the host: Conflict: When a MAC/IP was configured, the conflict was not known as the VNID was not mapped to the access port. After the VNID is mapped, if the same MAC/IP is present statically on some other port on the same VNID, then it is in conflict state. Learnt Conflict: When a MAC/IP was configured, the conflict was not known. However, it is now in conflict because the same MAC/IP is configured on an access port on VTEP1 and on an access port on VTEP2. Because the BGP session/tunnel was not up, the MAC/IP was not known to the other VTEP and the configuration was allowed. When the BGP session/tunnel comes up and it finds such a conflicted route, it marks the state as Learnt Conflict. Inactive: Configured but not operating, such as when the port is not mapped to any VNID. The port is down and the ARP/ND cache is disabled. Active: Operating host MAC/IP.

show nvo vxlan tunnel

Use this command to view the source, destination, and status of the VxLAN tunnel entries.

Command Syntax

```
show nvo vxlan tunnel
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show nvo vxlan tunnel` command.

```
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source Destination      Status Up/Down Update
================================================
1.1.1.1 2.2.2.2          Installed 00:00:20 00:00:20
Total number of entries are 1
```

Table 1-94 explains the output fields.

Table 1-94: VxLAN tunnel fields

Field	Description
Source	Tunnel source IP address.
Destination	Tunnel destination IP address.
Status	Installed: Tunnel Installed in the hardware and operating. Resolved: Tunnel destination IP is reachable, but VxLAN tunnel not installed in hardware. Therefore, not operating. Unresolved: Tunnel destination IP not reachable because L3 route is down.
Up/Down	When the tunnel came up or went down
Update	When the tunnel was last updated
Total number of entries	The total number of entries listed.

show running-config nvo vxlan

Use this command to display the current running configuration of VxLANs.

Command Syntax

```
show running-config nvo vxlan
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version before OcNOS version 1.3.

Example

```
#sh running-config  nvo vxlan
!
evpn vxlan multihoming enable
!
evpn esi hold-time 100
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 2.2.2.2
!
nvo vxlan mac-ageing-time 10
!
nvo vxlan id 10 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrfred
!
nvo vxlan access-if port-vlan xe13 10
 no shutdown
 map vnid 10
 mac 0000.0000.2222  ip 12.12.12.2
!
nvo vxlan access-if port-vlan xe17 10
 no shutdown
 map vnid 10
 mac 0000.0000.bbbb  ip 11.11.11.1
!
nvo vxlan access-if port-vlan xe17 30
 no shutdown
 map vnid 10
 mac 0000.1111.2222
!
nvo vxlan access-if port-vlan xe1 11
```

```
 description member-port xe1 with vlan 11
 no shutdown
 map vnid 10
!
nvo vxlan access-if port-vlan xe1 10
 no shutdown
 map vnid 10
!
nvo vxlan access-if port-vlan xe1 12
 no shutdown
 map vnid 10
!
```

show evpn multi-homing all

Use this command to display the multi-homed VTEP details.

Command Syntax

```
show evpn multi-homing all
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show evpn multi-homing all
ESI                             Access-IF    PE-IP-ADDRESS
============================================================
00:00:11:22:33:44:55:66:77:88  ce21/1       1.1.1.1
00:00:11:22:33:44:55:66:77:88  ----         2.2.2.2
Total number of entries are 2
```

Table 1-95 explains the output fields.

Table 1-95: show evpn multi-homing all output details

Field	Description
ESI	An Ethernet segment has an unique nonzero identifier, called the Ethernet segment identifier (ESI). The ESI is encoded as a 10-octet integer that identifies this segment. When manually configuring an ESI value, the most significant octet, known as the type byte, must be 00. When a single-homed CE device is attached to an Ethernet segment, the entire ESI value is zero.
Access-IF	Map the access port ce21/1 for evpn.
PE-IP-ADDRESS	Address of the provider edge router in the interface.

show evpn multihoming-status

Use this command to display the status of multihoming on a VTEP.

Command Syntax

```
show evpn multihoming-status
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show evpn multihoming-status
Multihoming is ACTIVE in Hardware
```

show nvo vxlan route-count

Use this command to display the VXLAN active route (MAC-IP and MAC-only) count information.

Command Syntax

```
show nvo vxlan route-count (|vnid <1-16777215>)
```

Parameters

<1-16777215>	Range supported for VNID

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and modified to include the GW-IPv4, and Prefix IPv4 in OcNOS version 1.3.5.

Example

```
#show nvo vxlan  route-count
VXLAN Active route count information
====================================
Max route count   : 32768
Active route count: 0

-------------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
-------------------------------------------
 100      0        0        0        0
 10       0        0        1        0

Total number of entries are 2
```

Table 1-96 explains the output fields.

Table 1-96: show nvo vxlan route-count output details

Field	Description
Max route count	Maximum number of route count in vxlan.
Active route count	Number of active route count in the interface.
VNID	VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Total	Total number of entries for the interface.
MACONLY	The MAC-only route for the local interface appears in the VXLAN instance route table.
MACIPv4	IPv4 media access control (MAC) address for a default virtual gateway.
MACIPv6	IPv6 media access control (MAC) address for a default virtual gateway.

show nvo vxlan vni-name

Use this command to display the vxlan results based on vni-name.

Command Syntax

```
show nvo vxlan vni-name (WORD)
```

Parameters

WORD	VXLAN id name

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan vni-name SITEA-PRO
VXLAN Information
=================
Codes: NW - Network Port
AC - Access Port
(u) - Untagged
VNID Vni-name Type Interface ESI Vlan DF-Status Src-addr Dst-addr
_____________________________________________________________________________________
_____________________________
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.8
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.9
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.3.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.1.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.5.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.1
1 SITEA-PRO AC xe7 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 1010 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 2020 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 200 ------ ---- ----
1 SITEA-PRO AC xe8 — Single Hommed port — ---- ------ ---- ----
1 SITEA-PRO AC po2 — Single Hommed port — ---- ------ ---- ----
Total number of entries are 16
```

shutdown

Use this command to administratively shut down an NVO access interface.

Use the no form of this command to start an NVO access interface.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

The NVO access interface is running by default.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#shutdown
(config-nvo-acc-if)#exit
```

vxlan host-reachability-protocol evpn-bgp

Use this command to set the host reachable protocol to Ethernet-VPN over BGP. This defines BGP as the mechanism for host reachability advertisement.

Use use the no form of this command to remove Ethernet-VPN as the host reachable protocol.

Command Syntax

```
vxlan host-reachability-protocol evpn-bgp NAME
no vxlan host-reachability-protocol evpn-bgp
```

Parameters

NAME	Name of the VRF to carry VNID routes

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#nvo vxlan id 3 ingress-replication inner-vid-disabled
(config-nvo)#vxlan host-reachability-protocol evpn-bgp Blue
```

CHAPTER 2 VXLAN Quality of Service Commands

This chapter describes the VXLAN commands for QoS (Quality of Service):

clear nvo vxlan tunnels

Use this command to clear the nvo vxlan tunnels to re-establish the tunnel after mapping/un-mapping the QoS profile to vxlan tunnel.

Command Syntax

```
clear nvo vxlan tunnels
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear nvo vxlan  tunnels
```

cos queue

Use this command to configure user defined mapping for cos and queue.

Use the no form of this command to remove the mapping.

Command Syntax

```
cos <0-7> queue <0-7>
no cos <0-7>
```

Parameters

cos	COS
queue	Queue number

Default

By default, the VXLAN multi-homing hardware-profile is disabled.

Command Mode

QoS config mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile cos-to-queue ac_port_ingress
(config-ingress-cos-map)#cos 1 queue 7
(config-ingress-cos-map)#no cos  1
```

dscp queue

Use this command to configure user defined mapping for DSCP to queue. This will be mapped with nvo VXLAN tunnel of remote VTEP.

Use the no form of this command to delete the mapping.

Command Syntax

```
dscp <0-63> queue <0-7>
no dscp <0-63>
```

Parameters

<0-63>	DSCP
<0-7>	Queue number

Command Mode

Ingress-dscp-map mode

Default

Default queue and cos value is one-one default mapping if it is not configured.

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile dscp-to-queue nw_profile
(config-ingress-dscp-map)#dscp 50 queue 1
(config-ingress-dscp-map)#no dscp 50
```

map qos-profile cos-to-queue

Use this command to map the cos-to-queue profile to vxlan access port on the local VTEP.

Use the no form of the command to remove the mapping.

Command Syntax

```
map qos-profile cos-to-queue NAME
```

Parameters

NAME	QoS profile name for access port mapping

Default

None

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
(config)#nvo vxlan access-if port-vlan xe1 10
(config-nvo-acc-if)#map qos-profile cos-to-queue ac_port_ingress
(config-nvo-acc-if)#no map qos-profile cos-to-queue ac_port_ingress
```

map qos-profile queue-color-to-cos

Use this command to map the queue-color-to-cos profile to vxlan access port on the remote VTEP.

Use the no form of the command to remove the mapping.

Command Syntax

```
map qos-profile queue-color-to-cos NAME
```

Parameters

NAME	QoS profile name for access port mapping

Default

None

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
(config)#nvo vxlan access-if port-vlan xe2 10
(config-nvo-acc-if)#map qos-profile queue-color-to-cos ac_profile
(config-nvo-acc-if)#no map qos-profile queue-color-to-cos ac_profile
```

nvo vxlan tunnel qos-map-mode cos-dscp

Use this command to map QoS profile for network side to nvo vxlan tunnel. For outgoing/incoming traffic, you need to provide the direction with the keyword `egress`/`ingress`.

Use the `no` form of this command to delete the mapping.

You must give the clear nvo vxlan tunnels command to do the network port setting for QoS profile mapped.

Command Syntax

```
nvo vxlan tunnel qos-map-mode cos-dscp (ingress|egress) NAME
no nvo vxlan tunnel qos-map-mode cos-dscp (ingress|egress)
```

Parameters

`NAME`	QoS profile name for network side
`ingress`	Ingress direction
`egress`	Egress direction

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress nw_profile
(config)#no nvo vxlan tunnel qos-map-mode cos-dscp egress
(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress nw_profile
(config)#no nvo vxlan tunnel qos-map-mode cos-dscp ingress
```

qos enable

Use this command to enable QoS globally. By enabling QoS, one-to-one (default) mapping of COS-to-queue is achieved in the hardware. By default, QoS is disabled.

To disable one-to-one mapping of COS-to-queue, use the `disable` form of the command.

Command Syntax

```
qos enable
qos disable
```

Parameters

None

Default

By default, QoS is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos enable
(config)#qos disable

#show running-config  qos
qos enable

(config)#qos disable
```

qos profile cos-to-queue

Use this command to configure cos-to-queue profile. This profile has to be mapped to VXLAN access port on the local VTEP.

Use the no form of this command to delete the qos profile.

Command Syntax

```
qos profile cos-to-queue NAME
```

Parameters

NAME	QoS profile name for cos-to-queue

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile cos-to-queue ac_port_ingress
(config)#no qos profile cos-to-queue ac_port_ingress
```

qos profile dscp-to-queue

Use this command to configure QoS profile for DSCP to Queue mapping. This profile will be mapped to nvo vxlan tunnel of remote VTEP. The created profile will support remarking of the data packets.

Use the no form of this command to delete the QoS profile

Command Syntax

```
qos profile dscp-to-queue NAME
```

Parameters

NAME	QoS profile name for ingress mapping for vxlan tunnel

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile dscp-to-queue nw_profile
(config-ingress-dscp-map)#exit
(config)#no qos profile dscp-to-queue nw_profile
(config)#
```

qos profile queue-color-to-cos

Use this command to configure queue-color-to-cos profile. This profile has to be mapped to VXLAN access port on remote VTEP.

Use the no form of this command to delete the qos profile.

Command Syntax

```
qos profile queue-color-to-cos NAME
```

Parameters

NAME	QoS profile name for queue-color-to-cos

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile queue-color-to-cos ac_profile
(config)#no qos profile queue-color-to-cos ac_profile
```

qos profile queue-color-to-dscp

Use this command to create a QoS profile queue-color-to-dscp. This profile will be mapped to nvo vxlan tunnel of local VTEP. The created profile supports remarking of the data packets.

Note: The profile name of "default" is not supported for VXLAN QoS.

Use the no form of this command to delete the profile.

Command Syntax

```
qos profile queue-color-to-dscp (NAME|default)
no qos profile queue-color-to-dscp (NAME|default)
```

Parameters

NAME	QoS profile name for queue-color-to-dscp

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile queue-color-to-dscp nw_profile
(config-egress-dscp-map)#exit
(config)#no qos profile queue-color-to-dscp nw_profile
```

queue cos

Use this command to configure user defined mapping for queue and cos.

Use the no form of this command to remove the mapping.

Command Syntax

```
queue <0-7> cos <0-7>
no queue <0-7>
```

Parameters

queue	Queue number
cos	COS

Default

Default queue and cos value is one-one default mapping if it is not configured.

Command Mode

QoS config mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile queue-color-to-cos ac_profile
(config-egress-cos-map)#queue 5 cos 2
(config-egress-cos-map)#no queue 5
```

queue dscp

Use this command to configure user-defined mapping for queue to DSCP. This will be mapped with nvo VXLAN tunnel of local VTEP.

Use the no form of this command to remove the queue-to-DSCP mapping.

Command Syntax

```
queue <0-7> dscp <0-63>
no queue <0-7>
```

Parameters

<0-7>	Queue number
<0-63>	DSCP

Default

Default queue and cos value is one-one default mapping if it is not configured.

Command Mode

Egress-dscp-map mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
(config)#qos profile queue-color-to-dscp nw_profile
(config-egress-dscp-map)# queue 1 dscp 63
(config-egress-dscp-map)#no queue 1
```

SECTION 17 Neighbor Discovery

Neighbor Discovery Configuration Guide

Contents

This document contains these chapters:

CHAPTER 1 Neighbor Discovery Configuration

This chapter provides an overview of Neighbor Discovery (ND) configuration.

The Address Resolution Protocol (ARP) translates network layer addresses into link-layer addresses. ARP converts a an IPv4 address to an Ethernet address (MAC address).

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery (ND) protocol. Neighbor Discovery operates at the link layer and is responsible for auto configuration of nodes, discovery of other nodes on the link, determining the link layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes.

ARP/Neighbor Discovery Operation

Neighbor Discovery module manages the ARP and IPv6 ND entries and provides information to other protocols, the forwarding module for their use, and reports state changes.

Neighbor Entry States

`INCOMPLETE`	Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.
`REACHABLE`	The neighbor is known to have been reachable recently.
`STALE`	The neighbor is no longer known to be reachable (not used by higher level protocol for reachable-time) but still valid and used for forwarding. Until any control packet is sent to the neighbor, no attempt will be made to verify its reachability.
`DELAY`	The neighbor is no longer known to be reachable, and traffic has recently been sent to the neighbor. Rather than probing the neighbor immediately, delay sending probes for a short while in order to give upper-layer protocols chance to provide reachability confirmation.
`PROBE`	The neighbor is no longer known to be reachable, andprobes are being sent to verify reachability.
`FAILED`	Address resolution is failed. No response received from the neighbor.

Below are few timers that control the above state transitions.

1. **reachable-time**
   The amount of time the entry is in REACHABLE state. The default value is 60 seconds.
   Once a neighbor is found, the entry is considered reachable for at least a random value between (A) & (3xA) where

   A = reachable-time /2

   Once entry reachability expires it moves to STALE state. The entry's reachability is extended if it receives positive feedback (ARP reply/NA).

2. **stale-time**
   Determines how often to check for stale neighbor entries. The default value is 1440 seconds.
   Once the stale-timer expires, the entry is marked for garbage collection.

3. **arp-ageing-time**
   The approximate amount of time ARP entry is valid. The default value is 1500 seconds. Ageing time is configured internally as below

   Age-time = reachable-time + stale-time

The garbage collector runs every 60 seconds once, to clean-up the entries which have crossed STALE timeout and FAILED entries. For improved performance benefits, following are the additional criteria for the neighbor entries to be garbage collected i.e. removal of the entry completely.

1. The garbage collector does not run if the total number of entries is less than 2048 that conveys some STALE, and FAILED entries still exist. The entry is refreshed ONLY when higher-level protocols use it.
2. The garbage collector is always run if we have number of entries more than 262144 for Ipv4 & 131072 for Ipv6.

The garbage collection triggers the refresh of neighbor entries which are marked to be garbage collected. A total of 3 retries with a 3 second interval is done to reach the neighbor, before declaring the neighbor as not reachable by the forwarder. During this retry period, neighbor entries are still in use for hardware forwarding. If the neighbor is still not reachable after retries (after 9 seconds), the neighbor entry is removed from hardware forwarding as well.

Configuring ARP for IPV4

The procedures in this section use the topology in Figure 1-131

Figure 1-131: ARP for IPV4

RTR1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#ip arp 2.2.2.3 0000.0000.0003`	Configure ARP entry for neighbor.
`(config)#exit`	Exit configure mode.

RTR2

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 2.2.2.3/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#ip arp 2.2.2.2 0000.0000.0004`	Configure ARP entry for neighbor.
`(config)#exit`	Exit configure mode.

Validation

```
#show arp

Flags: D - Static Adjacencies attached to down interface

Total number of entries: 2
Address          Age      MAC Address     Interface  State
10.12.17.1       00:00:29 44e4.d982.274a  eth0       REACHABLE
2.2.2.3             -     0000.0000.0003  xe1        PERMANENT
```

Configuring Neighbor Discovery for IPV6

The procedures in this section use the topology in Figure 1-132.

Figure 1-132: ND for IPv6

RTR1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 3ffe:506::1/48`	Configure IPv6 address on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# ipv6 neighbor 3ffe:506::2 xe1 0000.0000.0004`	Configure neighbor IPv6 address and MAC.
`(config)#exit`	Exit configure mode.

RTR2

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 3ffe:506::2/48`	Configure IPv6 address on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# ipv6 neighbor 3ffe:506::1 xe1 0000.0000.0003`	Configure neighbor IPv6 address and MAC.
`(config)#exit`	Exit configure mode.

Validation

```
#show ipv6 neighbors

R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe,
D - Delay, PR - Permanent
```

```
Flags: (D) - Static neighbors attached to down interface

IPv6 Neighbor Table for context default
Total number of entries:1
Address        Age       MAC Address     Source  Interface      State
3ffe:506::2      -       0000.0000.0004  static  xe1         PR
```

Neighbor Discovery Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Neighbor Discovery Commands

This chapter provides a description, syntax, and examples of the ND commands. It includes the following commands:

arp-ageing-timeout

Use this command to set the ARP aging timeout.

Note: The bridge aging time affects the ARP entries which are dependent upon the MAC addresses in hardware. If a MAC address ages out, it causes the corresponding ARP entry to refresh.

Use no form of this command to set the aging to its default value.

Command Syntax

```
arp-ageing-timeout <60-28800>
no arp-ageing-timeout
```

Parameter

<60-28800>	ARP aging timeout.

Default value

By default, the ARP aging timeout is 1500.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-ageing-timeout 5000
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-ageing-timeout
```

arp-reachable-time

Use this command to set the ARP reachable time.

Use no form of this command to set the reachable time to its default value.

Command Syntax

```
arp-reachable-time <10-3600>
no arp-reachable-time
```

Parameters

<10-3600>	Specify the ARP reachable time.

Default value

By default, arp-reachable-time is 60

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-reachable-time 120
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-reachable-time
```

clear arp

Use this command to clear dynamic ARP entries.

Command Syntax

```
clear arp (| A.B.C.D) (| vrf (all | VRFNAME | default))
clear arp IFNAME (| vrf (all | VRFNAME | default))
```

Parameters

`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear arp
#clear arp xe1
#clear arp 10.10.10.10
#clear arp vrf VRF1
```

clear ipv6 neighbors

Use this command to clear dynamic neighbor entries.

Command Syntax

```
clear ipv6 neighbors (|X:X::X:X) (|vrf (all | VRFNAME | default))
clear ipv6 neighbors IFNAME (|vrf (all | VRFNAME | default))
```

Parameters

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 neighbors
#clear ipv6 neighbors xe1
#clear ipv6 neighbors 2000::3
#clear ipv6 neighbors vrf VRF1
```

debug ip arp

Use this command to enable debugging for ARP events.

Note: Packet dumps are not available as part of debug logs. Use the `tcpdump` command to view packets.

Use the `no` parameter with this command to disable event debugging.

Command Syntax

```
debug ip arp event
no debug ip arp event
```

Parameters

`event`	ARP event debugging.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip arp event
```

debug ipv6 nd

Use this command to enable debugging for neighbor events.

Note: Packet dumps are not available as part of debug logs. Use the `tcpdump` command to view packets.

Use the `no` parameter with this command to disable event debugging.

Command Syntax

```
debug ipv6 nd event
no debug ipv6 nd event
```

Parameters

`event`	ND event debugging.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ipv6 nd event
```

ip arp

Use this command to create a static ARP entry.

Use the no parameter to remove the static ARP entry.

Command Syntax

```
ip arp A.B.C.D XXXX.XXXX.XXXX (alias|)
no ip arp A.B.C.D
```

Parameters

A.B.C.D	Specify the IP address of the ARP entry.
XXXX.XXXX.XXXX	Specify the MAC (hardware) address of the ARP entry.
alias	Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip arp 10.10.10.10 0000.0001.4566
(config)#no ip arp 10.10.10.10
```

ip arp vrf

Use this command to create a static ARP entry for the non-default VRF.

Note: This command is supported only for multiple VRF support.

Command Syntax

```
ip arp vrf NAME A.B.C.D XXXX.XXXX.XXXX (alias|)
```

Parameter

NAME	Specify VRF name to which entry need to be added.
A.B.C.D	Specify the IP address of the ARP entry.
XXXX.XXXX.XXXX	Specify the MAC (hardware) address of the ARP entry.
alias	Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip arp vrf VRF1 10.10.10.10 0000.0001.4566
```

ip proxy-arp

Use this command to enable the proxy ARP feature.

Use the no parameter to disable the proxy ARP feature.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameter

None

Default value

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip proxy-arp
(config-if)#no ip proxy-arp
```

ipv6 neighbor

Use this command to add a static neighbor entry.

Use the no form of this command to remove a static neighbor entry.

Command Syntax

```
ipv6 neighbor X:X::X:X IFNAME XXXX.XXXX.XXXX
no ipv6 neighbor X:X::X:X IFNAME
```

Parameter

X:X::X:X	Specify the neighbor's IPv6 address.
IFNAME	Specify the name of the interface.
XXXX.XXXX.XXXX	Specify the MAC hardware address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 neighbor 2000::3 xe1 0000.0002.3dc1
(config)#no ipv6 neighbor 2000::3 xe1
```

nd-ageing-timeout

Use this command to set the neighbor ageing timeout value.

Use no form of this command to set the ageing to its default value.

Command Syntax

```
nd-ageing-timeout <60-28800>
no nd-ageing-timeout
```

Parameters

<60-2880>	ND ageing timeout in seconds.
IFNAME	Specify the name of the interface.
XXXX.XXXX.XXXX	Specify the MAC hardware address.

Default value

By default, nd-ageing-timeout is 1500 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#nd-ageing-timeout 3600
(config-if)#no nd-ageing-timeout
```

nd-reachable-time

Use this command to set neighbor reachable time value.

Use no form of this command to set the reachable time to its default value.

Command Syntax

```
nd-reachable-time <10-3600>
no nd-reachable-time
```

Parameter

<10-3600>	ND reachable time in seconds.

Default value

By default, nd-reachable-time is 60 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#nd-reachable-time 300
(config-if)#no nd-reachable-time
```

no debug all

Use this command to disable all ARP and the neighbor debugging.

Command Syntax

```
no debug all
undebug all
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#no debug all
```

show arp

Use this command to display ARP entry information.

Command Syntax

```
show arp (| (A.B.C.D | detail | static) (| vrf (all | VRFNAME | default)))
show arp IFNAME (| vrf (all | VRFNAME | default))
show arp summary (|IFNAME) (| vrf (all | VRFNAME | default))
```

Parameters

`detail`	Display detailed information.
`static`	Display static ARP entries.
`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
VRFNAME	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age      MAC Address     Interface  State
10.12.18.1       00:00:18 44e4.d982.274b  eth0       REACHABLE
10.10.10.20      00:02:33 a8b1.d433.4140  xe1        STALE

#show arp summary vrf default

IP ARP Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```

Table 1-97 explains the show commmand output fields.

Table 1-97: show arp output details

Entry	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Interface	Logical address to connect the device over network.
State	INCOMPLETE – first ARP request sent, send ARP request. REACHABLE – normal expiration reset use counter. STALE – still usable; needs verification reset use counter; change state to delay. DELAY – schedule ARP request; needs verification reset use counter. PROBE – sending ARP request reset use counter. FAILED – no response received send ARP request. NOARP – normal expiration; never verified reset use counter. PERMANENT – never expires; never verified reset use counter. Note: INCOMPLETE/FAILED state entries are only cleared if the total number of ARP entries is more than 2048. It might take up to 60 seconds to clear the entries. This is an optimization to improve ND performance.

Network devices are considered adjacent if they can reach each other with a single hop. The summary command shows the count of the state of devices that are adjacencies.

Table 1-98 explains the show command output fields.

Table 1-98: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

show debugging ip arp

Use this command to display debugging information for ARP.

Command Syntax

```
show debugging ip arp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ip arp
ND IP Debugging status:
  ND ip arp event debugging is off
  ND ip arp packet debugging is off
```

show debugging ipv6 nd

Use this command to display debugging information for the neighbor.

Command Syntax

```
show debugging ipv6 nd
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ipv6 nd
ND IPV6 Debugging status:
  ND ipv6 event debugging is off
  ND ipv6 packet debugging is off
```

show ipv6 neighbors

Use this command to display the neighbor information.

Command Syntax

```
show ipv6 neighbors (| (X:X::X:X | detail | static) (| vrf (all | VRFNAME |
  default)))
show ipv6 neighbors IFNAME (| vrf (all | VRFNAME | default))
show ipv6 neighbors summary (| IFNAME) (| vrf (all | VRFNAME | default))
```

Parameters

`detail`	Show detail information of neighbor.
`static`	Static entry.
`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 neighbors

R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe,
D - Delay, PR - Permanent

Flags: (D) - Static neighbors attached to down interface

IPv6 Neighbor Table for context default
Total number of entries:2
Address         Age       MAC Address     Source  Interface      State
fe80::210:18ff:fe7f:f758
                00:43:04  0010.187f.f758  icmpv6  eth0             S
2000::5         00:55:25  0000.0001.0242  icmpv6  xe1              S

#show ipv6 neighbors summary

IPv6 Neighbors Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```

Table 1-99 shows the status codes displayed at the start of a route entry.

Table 1-99: status code output details

Status Code	Field	Description
R	Reachable	Normal expiration reset use counter.
I	Incomplete	First ARP request sent, send ARP request.
S	Stale	Still usable; needs verification reset use counter; change state to delay.
F	Failed	ARP requests response not received.
P	Probe	ARP request reset use counter.
D	Delay	Schedule ARP request; needs verification reset use counter.
PR	Permanent	Never expires; never verified reset use counter.

Table 1-100 explains the show command output fields.

Table 1-100: show ipv6 neighbors output details

Field	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Source	ARP request source in the interface.
Interface	Logical address to connect the device over network.
State	ARP request state that is being handled by the IPv6 neighbor session.

Table 1-101 explains the show command output fields.

Table 1-101: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

SECTION 18 Optical Line Termination

Optical Line Termination Configuration Guide

Contents

This document contains these chapters:

CHAPTER 1 OLT Configuration

Overview

The OcNOS optical line termination or terminal (OLT) device serves as an endpoint of a passive optical network (PON) of the service provider. OcNOS OLT supports XGS-PON which provides 10Gbps symmetric data transmission capability over the fiber network. The OLT allows the service provider to configure the optical network unit (ONU) and send specific traffic required for the service(s) to the subscribers.

Note: TIBIT OLT VM can be accessed by using switch management IP address with port number 2023 for telnet and 2022 for ssh connection.

OLT Configuration

User can create multiple OLT instances and enable the OLT.

```
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#pon-configuration
OcNOS(config-pon)#olt-id 0
OcNOS(config-pon-olt)# serial-number e8:b4:70:70:01:92
```

Note: The serial number of the TIBIT micro-plug can be found using "show pon olt mapping" CLI Serial Number configuration is required only for TIBIT OLT.

Use the OLT configuration to create multiple OLT instances and enable the OLT with 2 ONU provisioning modes as follows:

- Manual provisioning mode or pre-provisioning ONU mode
- Automatic provisioning mode

To enter into OLT configuration mode, execute the following commands:

Note: Currently one OLT (`OLT-ID 0`) instance is supported for ASXvOLT16 and 64 instances are supported for TIBIT OLT.

Manual Provisioning Mode

Use the CLI to configure the ONU provisioning mode as manual to the discovered and connected ONUs to the OLT system manually.

To set the OLT configuration in manual provisioning mode, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Enter PON configure mode
`(config-pon)# olt-id 0`	Input OLT instance Identifier
`(config-pon-olt)# onu-provisioning-type manual administrative-state up`	Configure manual ONU provisioning mode and enable OLT admin state
`(config-pon-olt)#exit`	Exit configure mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon olt 0

  admin-status:   UP
  oper-status:    UP
  onu-mode:       MANUAL_PROVISION
  dhcp-mode:      ON
  pon-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED
    ------------------------------------------------------
    pon0/0/1       DOWN          DOWN         -       XG-S
    pon0/0/2       DOWN          DOWN         AD      XG-S
    pon0/0/3       DOWN          DOWN         AD      XG-S
    pon0/0/4       DOWN          DOWN         AD      XG-S
    pon0/0/5       DOWN          DOWN         AD      XG-S
    pon0/0/6       DOWN          DOWN         AD      XG-S
    pon0/0/7       DOWN          DOWN         AD      XG-S
    pon0/0/8       DOWN          DOWN         AD      XG-S
    pon0/0/9       DOWN          DOWN         AD      XG-S
    pon0/0/10      DOWN          DOWN         AD      XG-S
    pon0/0/11      DOWN          DOWN         AD      XG-S
    pon0/0/12      DOWN          DOWN         AD      XG-S
    pon0/0/13      DOWN          DOWN         AD      XG-S
    pon0/0/14      DOWN          DOWN         AD      XG-S
    pon0/0/15      DOWN          DOWN         AD      XG-S
    pon0/0/16      DOWN          DOWN         AD      XG-S
  nni-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    NNI-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  FEC
    ------------------------------------------------------------
    nni0/0/1       UP            DOWN         PD      100G   OFF
    nni0/0/2       UP            DOWN         PD      100G   OFF
    nni0/0/3       UP            DOWN         PD      100G   OFF
    nni0/0/4       UP            UP           -       100G   OFF
#
```

Automatic Provisioning Mode

Use the CLI to configure the ONU provisioning mode as automatic to the discovered and connected ONUs to the OLT system automatically. The OLT automatically discovers the ONU(s) and program the default profiles.

To set the OLT configuration in automatic provisioning mode, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Enter PON configure mode
`(config-pon)# olt-id 0`	Input OLT instance Identifier
`(config-pon-olt)# onu-provisioning-type automatic administrative-state up`	Configure automatic ONU provisioning mode and enable OLT admin state
`(config-pon-olt)#exit`	Exit configure mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon olt 0

  admin-status:   UP
  oper-status:    UP
  onu-mode:       AUTOMATIC_PROVISION
  dhcp-mode:      ON
  pon-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED
    ------------------------------------------------------
    pon0/0/1       DOWN          DOWN         -       XG-S
    pon0/0/2       DOWN          DOWN         AD      XG-S
    pon0/0/3       DOWN          DOWN         AD      XG-S
    pon0/0/4       DOWN          DOWN         AD      XG-S
    pon0/0/5       DOWN          DOWN         AD      XG-S
    pon0/0/6       DOWN          DOWN         AD      XG-S
    pon0/0/7       DOWN          DOWN         AD      XG-S
    pon0/0/8       DOWN          DOWN         AD      XG-S
    pon0/0/9       DOWN          DOWN         AD      XG-S
    pon0/0/10      DOWN          DOWN         AD      XG-S
    pon0/0/11      DOWN          DOWN         AD      XG-S
    pon0/0/12      DOWN          DOWN         AD      XG-S
    pon0/0/13      DOWN          DOWN         AD      XG-S
    pon0/0/14      DOWN          DOWN         AD      XG-S
    pon0/0/15      DOWN          DOWN         AD      XG-S
    pon0/0/16      DOWN          DOWN         AD      XG-S
  nni-ports:
```

```
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    NNI-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  FEC
    ------------------------------------------------------------
    nni0/0/1       UP            DOWN         PD      100G   OFF
    nni0/0/2       UP            DOWN         PD      100G   OFF
    nni0/0/3       UP            DOWN         PD      100G   OFF
    nni0/0/4       UP            UP           -       100G   OFF
#
```

CHAPTER 2 PON Interface Configuration

Overview

The optical line termination (OLT) configuration includes the following two interfaces:

- PON — Use this interface to connect to ONUs.
- NNI — Use this interface to connect to core network.

The OLT PON interface connects the user and the ONUs. This PON interface is not visible until the OLT configuration is completed.

Note: The PON interface is down by default for ASXvOLT16 and it will be up by default for TIBIT OLT.

To configure the PON interface, execute the following commands:

`#configure terminal`	Enter configure mode.
`(config)# interface pon0/0/1`	Select an interface to configure and IFNAME
`(config-if)#no shut`	Set admin state of interface
`(config-if)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon olt 0 pon-port pon0/0/1

  admin-state:   UP
  oper-status:   UP
  speed:         XG-S

#show pon olt 0 pon-port brief

    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED
    ------------------------------------------------------
    pon0/0/1       UP            UP           -       XG-S
    pon0/0/2       DOWN          DOWN         AD      XG-S
    pon0/0/3       DOWN          DOWN         AD      XG-S
    pon0/0/4       DOWN          DOWN         AD      XG-S
    pon0/0/5       DOWN          DOWN         AD      XG-S
    pon0/0/6       DOWN          DOWN         AD      XG-S
    pon0/0/7       DOWN          DOWN         AD      XG-S
    pon0/0/8       DOWN          DOWN         AD      XG-S
    pon0/0/9       DOWN          DOWN         AD      XG-S
```

```
    pon0/0/10      DOWN          DOWN          AD      XG-S
    pon0/0/11      DOWN          DOWN          AD      XG-S
    pon0/0/12      DOWN          DOWN          AD      XG-S
    pon0/0/13      DOWN          DOWN          AD      XG-S
    pon0/0/14      DOWN          DOWN          AD      XG-S
    pon0/0/15      DOWN          DOWN          AD      XG-S
    pon0/0/16      DOWN          DOWN          AD      XG-S
#
```

NNI Interface Configuration

OLT NNI interface connects to the core network. The NNI port supports 40G and 100G speed interfaces. The user can configure the speed of the NNI interface. The Forward Error Correction (FEC) is disabled for 100G interface by default while it is not applicable for 40G interface.

Note: The NNI interface by default enables the admin state to up and supports100G speed for ASXvOLT16 only. Speed change command is not applicable to NNI interface on TIBIT OLT and default speed is 10G.

To configure the speed of the NNI interface, execute the following commands:

`#configure terminal`	Enter configure mode
`(config)# interface nni0/0/1`	Select an interface to configure and IFNAME
`(config-if)# speed 40g`	Set interface port speed to 40G
`(config-if)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output on ASXvOLT16.

```
#show pon olt 0 nni-port nni0/0/1

  admin-state:   UP
  oper-status:   UP
  speed:         40G
  fec:           OFF
#
```

Execute the `show` command to verify the output on TIBIT OLT.

```
#show pon olt 0 nni-port nni0/0/1

 admin-state:UP
 oper-status:UP
 speed:10G
#
```

FEC Configuration

OLT supports Forward Error Correction (FEC) with 100G speed for the NNI interface.

Note: FEC config for NNI interface is not supported on TIBIT OLT.

`#configure terminal`	Enter configure mode
`(config)# interface nni0/0/4`	Select an interface to configure and IFNAME
`(config-if)# FEC on`	Enable FEC
`(config-if)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` commands to verify the output.

```
#show pon olt 0 nni-port brief

    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    NNI-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  FEC
    ------------------------------------------------------------
    nni0/0/1       UP            DOWN         PD      100G   OFF
    nni0/0/2       UP            DOWN         PD      100G   OFF
    nni0/0/3       UP            DOWN         PD      100G   OFF
    nni0/0/4       UP            UP           -       100G   ON

#show pon olt 0 nni-port nni0/0/4

  admin-state:   UP
  oper-status:   UP
  speed:         100G
  fec:           ON
#
```

CHAPTER 3 ONU-Profile Configuration

Overview

Use ONU Profile to create a `onu-profile` and associate with the ONU. The ONU-profile configuration allows the OLT user to configure one GEM-port to one T-Cont and assign this to logical UNI-Port. The ONU-profile associates with the actual ONU.

OLT allows to configure the profile-name of the `onu-profile` with maximum of 32-characters.

To configure a ONU profile, execute the following commands:

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# onu-profile profile-name Sample1`	Input ONU profile name

UNI Port-ID and GEM port Configuration

OLT allows user to create logical UNI Port-ID and GEM port to send upstream and downstream traffic of a specific p-bit.

To configure a UNI and GEM port, execute the following commands:

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Enter PON configure mode
`(config-pon)# onu-profile profile-name onu_prof1`	Configure ONU profile-name
`(config-pon-op)# uni port-id 0`	Input UNI logical port id and UNI port ID value
`(config-pon-op-uni)#gem-port-name GEM0 p-bits 0 upstream-priority-queue 0 downstream-priority-queue 0`	Input Gem port identifier, GEM port name, p-bits range, upstream priority queue, upstream priority queue
`(config-pon-op-uni)#exit`	Exit configuration mode

T-CONT Configuration

The T-Cont configuration allows user to configure T-Cont with unique name and associate the GEM-Port to the T-Cont.

To configure the T-CONT interface, execute the following commands:

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# onu-profile profile-name Sample1`	Input ONU profile name
`(config-pon-op)# t-cont TC01`	Input T-Cont name
`(config-pon-op-tcont)#gem-port-name GEM0`	Input Gem port identifier, gem-port name
`(config-pon-op-tcont)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon onu-profile brief

  default_onu_profile
  Sample1

#show pon onu-profile Sample1

  onu-tconts:
    T-CONT-NAME
    -----------
    TC01
  gem-ports:
    GEM-PORT-NAME        TCONT-NAME           UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------------------------
    GEM0                 TC01                 0             0        0       0
  uni-logic-ports:
    UNI-LOGIC-PORT-ID
    -----------------
    0
#
```

Note: Associate only one GEM-Port to one T-Cont.

Logical UNI Port-ID is linked to Physical UNI port ID.

Note: Maximum 8 T-Conts are supported per ONU.

CHAPTER 4 Translation-Profile Configuration

Overview

Use Translation Profile to filter the ingress traffic based on specific vlan-type traffic type and allow only specific traffic for services.

Untagged Traffic Classification Configuration

To configure a translation profile with untagged classification, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# translation-profile profile-name Untag_Sample`	Create a translation profile name
`((config-pon-tp)#classification`	Enter match rule for translation profile name.
`(config-pon-tp-classification)#vlan-type untagged`	Configure untag vlan-type match rule
`(config-pon-tp-tcont)#exit`	Exit configuration mode
`(config-pon-tp)#treatment`	Apply action on configured match rule
`(config-pon-tp-treatment)#p-bits 0 operation none`	Configure the outgoing vlan parameters, output p-bits, and operation to perform
`(config-pon-tp-treatment)#exit`	Exit configuration mode

UNI Port-ID and GEM port Configuration

The OLT allows user to create logical UNI port identifier and GEM port identifier to send upstream and downstream traffic of a specific p-bit.

To configure a logical link between UNI and GEM port, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Enter PON configure mode
`(config-pon)# onu-profile profile-name onu_prof1`	Configure ONU profile-name
`(config-pon-op)# uni port-id 0`	Input UNI logical port id and UNI port ID value
`(config-pon-op-uni)#gem-port-name GEM0 p-bits 0 upstream-priority-queue 0 downstream-priority-queue 0`	Inpute GEM port identifier, GEM port name, p-bits range value, upstream priority queue value.
`(config-pon-op-uni)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon translation-profile Untag_Sample

  ------------------------------------------------------------------------------
                            |         CLASSIFICATION          |     TREATMENT
  TRANS-PROFILE-NAME        | VLAN-TYPE      VLAN-ID  P-BITS | OPERATION    P-BITS
  ------------------------------------------------------------------------------
  Untag_Sample                UNTAGGED       0        0        NONE         0
#
```

Tagged Traffic Classification Configuration

To configure a translation profile with tagged classification, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# translation-profile profile-name Tag_Sample`	Enter translation profile name
`((config-pon-tp)#classification`	Enter match rule for translation profile name
`(config-pon-tp-classification)# vlan-type tagged vlan-id 10 p-bits 0`	Configure tagged vlan-type match rule. Input vlan type tagged, vlan identifier, p-bits range value
`(config-pon-op-tcont)#exit`	Exit configuration mode
`(config-pon-tp)#treatment`	Apply action on configured match rule
`(config-pon-tp-treatment)#p-bits 0 operation remove-vlan`	Configure the outgoing vlan parameters, output p-bits, and operation to perform
`(config-pon-tp-treatment)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon translation-profile Tag_Sample

  ------------------------------------------------------------------------------
                            |         CLASSIFICATION          |     TREATMENT
  TRANS-PROFILE-NAME        | VLAN-TYPE      VLAN-ID  P-BITS | OPERATION    P-BITS
  ------------------------------------------------------------------------------
  Tag_Sample                  TAGGED         10       0        REMOVE_VLAN  0
#
```

Priority-Tagged Traffic Classification Configuration

To configure a translation profile with priority tagged classification, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# translation-profile profile-name PriorityTag _Sample`	Enter translation profile name
`((config-pon-tp)#classification`	Enter match rule for translation profile name
`(config-pon-tp-classification)# vlan-type prioritytagged p-bits 0`	Configure priority tagged vlan-type match rule. Input vlan type priority tagged, p-bits range value
`(config-pon-tp-tcont)#exit`	Exit configuration mode
`(config-pon-tp)#treatment`	Apply action on the configured match rule
`(config-pon-tp-treatment)#p-bits 0 operation remove-vlan`	Configure the outgoing vlan parameters, output p-bits, and operation to perform
`(config-pon-tp-treatment)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon translation-profile PriorityTag_Sample

  ------------------------------------------------------------------------------
                            |         CLASSIFICATION         |     TREATMENT
  TRANS-PROFILE-NAME        | VLAN-TYPE      VLAN-ID  P-BITS | OPERATION    P-BITS
  ------------------------------------------------------------------------------
  PriorityTag_Sample          PRIORITYTAGGED 0        0        REMOVE_VLAN  0
#
```

Note: Remove-Vlan operation is not supported for `Vlan-Type Untagged.`

None operation is not supported for `Vlan-Type Tagged` and `Priority Tagged`.

CHAPTER 5 QoS-Profile Configuration

Overview

Use Quality of Service (Qos) profile to configure a generic mechanism to describe the QoS parameters such as Committed, Peak Information Rate and Burst Size for upstream and downstream data traffic.The OLT allows user to configure the CIR and PIR parameters in kbps, mbps and gbps units.

To configure QoS parameters, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# qos-profile profile-name QoS_Sample`	Configure qos-profile name
`(config-pon-qp)# upstream`	Enter QOS upstream config mode
`(config-pon-qp-upstream)# cir 100 mbps pir 101 mbps`	Input Committed Information Rate units value, Peak Information Rate units value
`(config-pon-qp-upstream)#exit`	Exit configuration mode
`(config-pon-qp)#downstream`	Enter QOS downstream config mode
`(config-pon-qp- downstream)# cir 150 mbps pir 151 mbps pbs 1 mbytes`	Specify Committed Information Rate units value, Peak Information Rate units value
`(config-pon-qp- downstream)#exit`	Exit configuration mode

Note: Ensure the CIR value is less than PIR value by at least 128 kbps.

The maximum CIR varies based on the number of ONUs connected.

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` commands to verify the output.

```
#show pon qos-profile brief

  default_qos_profile
  QoS_Sample


#show pon qos-profile QoS_Sample

  *CIR - Committed Information Rate
  *PIR - Peak Information Rate
  *PBS - Peak Burst Size

  dn-stream-rate-policer:
    CIR      CIR_UNITS      PIR      PIR_UNITS      PBS      PBS_UNITS
    ------------------------------------------------------------------
```

```
    150         mbps        151         mbps        1           mbytes
  up-stream-rate-policer:
    CIR      CIR_UNITS      PIR      PIR_UNITS
    ----------------------------------------
    100         mbps        101         mbps
#
```

CHAPTER 6 ONU Configuration

Overview

Configure the user end ONU equipment using the ONT management control interface (OMCI) of the OLT. The ONU is configured manually in manual mode where as it is configured automatically in the automatic mode after the ONC is discovered. Refer to Chapter 2, *PON Interface Configuration*.

To configure ONU, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# onu-id 0`	Input ONU identifier
`(config-pon-onu)# olt olt-id 0 pon-port pon0/0/1 serial-number 414C5048E3BB87DE profile-name Sample1`	Input optical line termination Identifier value, PON port interface for ONU, PON port serial number for ONU, corresponding ONU profile name

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon onu brief

  ONU-ID     OLT-ID   ADMIN-STATE OPER-STATUS     PON-PORT     SERIAL#
  ------------------------------------------------------------------------
  0          0        UP          UP              pon0/0/1
414C5048E3BB87DE(ALPHE3BB87DE)
#show pon onu 0
  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB87DE(ALPHE3BB87DE)
  onu-profile-name:  Sample1
  admin-state:       UP
  oper-status:       UP
  uni-ports:         5
  tcont-maps:
    ALLOC-ID      TCONT-NAME            PON-PORT-NAME
    ------------------------------------------------
    1024          TC01                  pon0/0/1
  gem-port-maps:
    GEM-PORT-ID   GEM-PORT-NAME         PON-PORT-NAME
    ------------------------------------------------
    1024          GEM0                  pon0/0/1
  onu-flow-list:
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   CONFIG-IND
```

```
    ------------------------------------------------
    0             LOCKED        ENABLED       Unknown
#
```

ONU UNI PORT Configuration

The ONU UNI Port is a physical port in the ONU equipment.The OLT user has the control over the administrative status of the UNI port.

To configure UNI port, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# onu-id 0`	Input ONU identifier
`(config-pon-onu)# uni-port-id 0`	Input UNI port identifier
`(config-pon-onu-uni)#administrative-state unlock`	Unlock the physical port usage
`(config-pon-onu-uni)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon onu 0

  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB87DE(ALPHE3BB87DE)
  onu-profile-name:  Sample1
  admin-state:       UP
  oper-status:       UP
  uni-ports:         5
  tcont-maps:
    ALLOC-ID      TCONT-NAME            PON-PORT-NAME
    ------------------------------------------------
    1024          TC01                  pon0/0/1
  gem-port-maps:
    GEM-PORT-ID   GEM-PORT-NAME         PON-PORT-NAME
    ------------------------------------------------
    1024          GEM0                  pon0/0/1
  onu-flow-list:
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   CONFIG-IND
    ------------------------------------------------
    0             UNLOCKED      ENABLED       1G Ethernet full duplex
#
```

CHAPTER 7 Flow Configuration

Overview

Use Flow configuration to provision a specific VLAN type required for the subscriber service(s). The OLT user can configure one or more flow per UNI port with different S+C VLAN combinations.

Note: The flow parameters for active flows cannot be updated on the fly. To update the flow, delete it and create it afresh with new values.

Topology

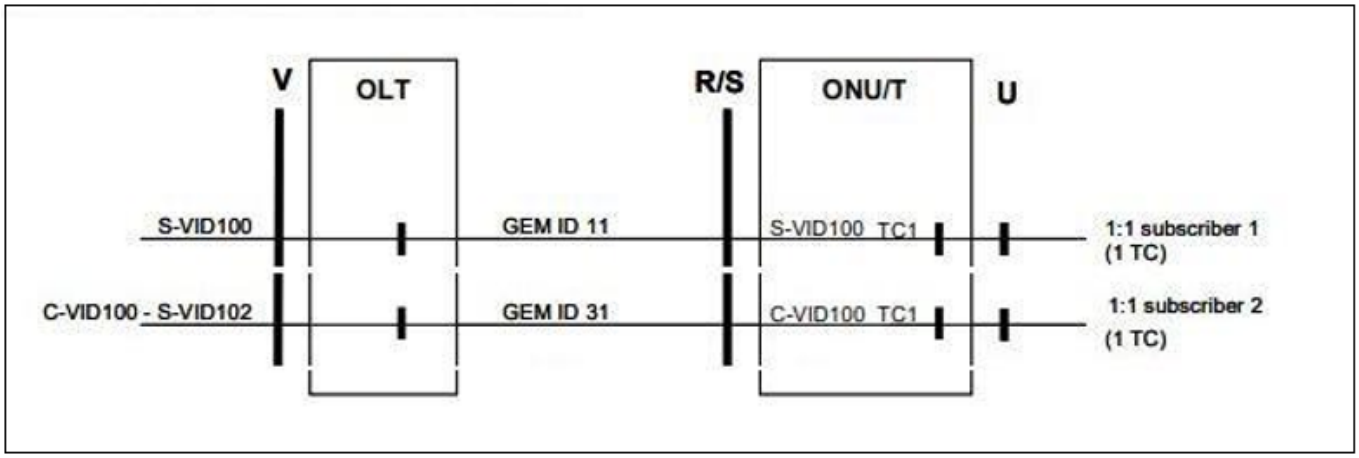


Figure 7-133: Subscriber Service Flow Configuration

S-Vlan Flow Configuration

Use S-Vlan flow configuration to allow the Untag or Tagged or Priority-Tagged traffic from user to S-Tag traffic.

To configure S-Vlan flow, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# flow-id 0`	Input Flow identifier
`(config-pon-flow)#uni`	Enter UNI config flow mode
`(config-pon-flow-uni)#onu-id 0 uni-port-id 0 vlan-tag 100 translation-profile-name Untag_Sample`	Input ONU id, UNI port id, vlan-tag, translation profile name for flow
`(config-pon-flow-uni)#exit`	Exit configuration mode
`(config-pon-flow)#nni`	Enter NNI config flow mode

(config-pon-flow-nni)#olt-id 0 nni-port-name nni0/0/1	Input OLT id, NNI port name for flow
(config-pon-flow-nni)#exit	Exit configuration mode
(config-pon-flow)#qos	Enter QoS config flow mode
(config-pon-flow-qos)#qos-profile-name QoS_Sample	Input QoS Profile name
(config-pon-flow-qos)#exit	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the show command to verify the output.

```
#show pon flow brief

    FLOW-ID       FLOW-OPER-STATUS
    ------------------------------
    0             UP

#show pon flow 0

  flow-oper-status:     UP
  pon-port:             pon0/0/1
  uni-end:
    onu-id:             0
    uni-port-id:        0
    trans-profile-name: Untag_Sample
    onu-vlan-tag:       100
  nni-end:
    olt-id:             0
    nni-port-name:      nni0/0/1
    olt-vlan-tag:       0
  qos:
    qos-profile-name:   QoS_Sample
  tcont:
    T-CONT-NAME
    -----------
    TC01

  gemport:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    GEM0                 0             0        0       0
  acl:
    id     priority direction  action      protocol remote-port   remote-ip
    ------------------------------------------------------------------------

#
```

S+C-Vlan Flow Configuration

Use S+C-Vlan flow configuration to allow the Untag or Tagged or Priority-Tagged traffic from user to S+C-Tag traffic.

To configure S+C Vlan, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# flow-id 1`	Input Flow identifier
`(config-pon-flow)#uni`	Enter UNI config flow mode
`(config-pon-flow-uni)#onu-id 0 uni-port-id 0 vlan-tag 100 translation-profile-name Tag_Sample`	Input ONU id, UNI Port id, vlan-tag, translation profile name for flow
`(config-pon-flow-uni)#exit`	Exit configuration mode
`(config-pon-flow)#nni`	Enter NNI config for flow mode
`(config-pon-flow-nni)#olt-id 0 nni-port-name nni0/0/1 vlan-tag 102`	Input OLT id, NNI port name, vlan-tag for flow
`(config-pon-flow-nni)#exit`	Exit configuration mode
`(config-pon-flow)#qos`	Enter QoS config for flow mode
`(config-pon-flow-qos)#qos-profile-name QoS_Sample`	Input QoS Profile name
`(config-pon-flow-qos)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon flow brief

    FLOW-ID       FLOW-OPER-STATUS
    ------------------------------
    0             UP
    1             UP

#show pon flow 1

  flow-oper-status:     UP
  pon-port:             pon0/0/1
  uni-end:
    onu-id:             0
    uni-port-id:        0
    trans-profile-name: Tag_Sample
    onu-vlan-tag:       100
  nni-end:
    olt-id:             0
    nni-port-name:      nni0/0/1
```

```
    olt-vlan-tag:       102
  qos:
    qos-profile-name:   QoS_Sample
  tcont:
    T-CONT-NAME
    -----------

    TC01
  gemport:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    GEM0                 0             0        0       0
  acl:
    id     priority direction  action      protocol remote-port   remote-ip
    ------------------------------------------------------------------------
```

CHAPTER 8 ACL Configuration

Overview

An access control list (ACL) consists a list of access control entries (ACE) which specifies the access privilege to allow or deny the flow service. The data packet arrives at the device is compared against each ACE, in the order defined in the ACL, until a match is found. When the device exhaust the ACE list and found no match, then it allows the data packet. If a match is found, then stops checking the access control list and deny the data packet.

Use ACL Configuration to specify ACL rule for each flow services. The ACL configuration can be used in Flow service only.

To configure ACL list, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# flow-id 0`	Input flow identifier
`(config-pon-flow)#acl`	Enter ACL config flow mode
`(config-pon-flow-acl)#pon-acl-id 10 priority 10 action drop direction upstream remote-ip 10.10.10.10 protocol any`	Input ACL rule identifier, priority, action for matching ACL rule, direction for ACL rule criteria, upstream destination IP for ACL rule criteria, Layer 4 protocol for ACL rule criteria
`(config-pon-flow-acl)#pon-acl-id 20 priority 20 action allow direction downstream remote-ip 20.20.20.20 protocol any`	Input ACL rule identifier, priority, action for matching ACL rule, direction for ACL rule criteria, downstream source IP for ACL rule criteria, Layer 4 protocol for ACL rule criteria
`(config-pon-flow-acl)#exit`	Exit configuration mode

Note: Remote-port parameter is optional which results in performing specific ACL rule action if packet matches with protocol-port.

Note: ACL configuration is not supported for TIBIT OLT.

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon acl all

==================== Flow ID: 0 ====================
    id     priority direction  action      protocol remote-port   remote-ip
    ------------------------------------------------------------------------
    10     10       upstream   drop        any      -             10.10.10.10
    20     20       downstream allow       any      -             20.20.20.20

#show pon flow 0

  flow-oper-status:     UP
  pon-port:             pon0/0/1
  uni-end:
    onu-id:             0
```

```
    uni-port-id:        0
    trans-profile-name: default_translation_profile
    onu-vlan-tag:       41
  nni-end:
    olt-id:             0
    nni-port-name:      nni0/0/1
    olt-vlan-tag:       0
  qos:
    qos-profile-name:   default_qos_profile
  tcont:
    T-CONT-NAME
    -----------
    default_tcont
  gemport:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    default_gemport      0             0        1       1
  acl:
    id     priority direction  action      protocol remote-port   remote-ip
    ------------------------------------------------------------------------
    10     10       upstream   drop        any      -             10.10.10.10
    20     20       downstream allow       any      -             20.20.20.20

#
```

CHAPTER 9 DHCP Configuration

Overview

Use the DHCP configuration to enable or disable the DHCP service. The OLT supports Layer2 DHCP relay with Option-82 (Agent Circuit ID) to forward the DHCP packets from the subscribers to the DHCP server.

DHCP Enable/Disable

Execute the following commands to enable or disable the DHCP service.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# olt-id 0`	Input OLT Identifier
`(config-pon-olt)# dhcp on`	Enable or disable DHCP relay option-82 for OLT. Use on/off values
`(config-pon-olt)#exit`	Exit configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon olt 0

  admin-status:   UP
  oper-status:    DOWN
  onu-mode:       MANUAL_PROVISION
  dhcp-mode:      ON
  pon-ports:
  nni-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)
```

CHAPTER 10 OLT Statistics

Overview

The OLT configuration supports to view the statistics of NNI, PON and UNI interfaces.The PON or NNI statistics displays TX, RX bytes, TX, RX Packets, TX, RX Drop packets count for Error packets.

Note: Tx drop packet count is not supported for PON and NNI port in TIBIT OLT.

NNI Statistics

The NNI Port statistics displays TX-Bytes, RX-Bytes, TX- PKTS, RX- PKTS, TX-DROP-PKTS, RX-DROP-PKTS counters.

Execute the following commands to display statistics.

```
#show pon statistics nni-port brief

  NNI port: nni0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/2
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/3
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/4
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0


#show pon statistics nni-port nni0/0/1
  NNI port: nni0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
#
```

PON Statistics

The PON Port statistics displays TX-Bytes, RX-Bytes, TX- PKTS, RX- PKTS, TX-DROP-PKTS, RX-DROP-PKTS counters.

Execute the following commands to display statistics.

```
#show pon statistics pon-port brief
```

```
PON port: pon0/0/1
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  361         17328         355         17040         0           0
PON port: pon0/0/2
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/3
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/4
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/5
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/6
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/7
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/8
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/9
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/10
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/11
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/12
  RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
  ------------------------------------------------------------------------
  0           0             0           0             0           0
PON port: pon0/0/13
```

```
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  PON port: pon0/0/14
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  PON port: pon0/0/15
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  PON port: pon0/0/16
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0

#show pon statistics pon-port pon0/0/1
  PON port: pon0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    361         17328         355         17040         0           0
#
```

UNI Statistics

The UNI port statistics displays UPSTREAM and DOWNSTREAM packets and bytes counters.

Execute the following commands to display statistics.

```
#show pon statistics onu 0 uni-port 0

  UNI port: 0, ONU-ID: 0
    PACKETS         BYTES           DIRECTION
    ----------------------------------------
    4010618         1848817297      UPSTREAM
    15              1230            DOWNSTREAM
#
```

DHCP Statistics

The DHCP statistics displays DHCP packets counter details.

Execute the following commands to display statistics

```
#show pon statistics dhcp option-82-pkts

DHCP Option-82 statistics:
INSERTED REMOVED INSERTION-ERROR DELETION-ERROR
---------------------------------------------------------------
27    0       0               0
#show pon statistics dhcp
DHCPDISCOVER : 27
```

```
DHCPOFFER : 0
DHCPREQUEST : 0
DHCPDECLINE : 0
DHCPACK : 0
DHCPNAK : 0
DHCPRELEASE : 0
DHCPINFORM : 0
DHCPV6_SOLICIT : 0
DHCPV6_ADVERTISE : 0
DHCPV6_REQUEST : 0
DHCPV6_CONFIRM : 0
DHCPV6_CONFIRM : 0
DHCPV6_RENEW : 0
DHCPV6_REBIND : 0
DHCPV6_REPLY : 0
DHCPV6_RELEASE : 0
DHCPV6_DECLINE : 0
DHCPV6_RECONFIGURE : 0
DHCPV6_INFORMATION_REQUEST : 0
DHCP_INVALID_REQ : 0
DHCP_INVALID_RES : 0
DHCP_INVALID_V6 : 27
DHCP_PKT_RCV : 0
DHCP_PKT_RCV_ERROR : 27
DHCP_PKT_SENT : 0
DHCP_PKT_SEND_ERROR : 27
DHCP_OPTION82_INSERTED : 0
DHCP_OPTION82_REMOVED : 0
DHCP_OPTION82_INSERTION_ERROR : 0
DHCP_OPTION82_DELETION_ERROR : 0
DHCP_INVALID_PACKET : 0
DHCP_FLOW_NOT_FOUND : 0
DHCP_IF_NOT_FOUND : 0
#
```

CHAPTER 11 Logging and Debugging

Overview

Use the OLT logging option to set the console log level and enable PON log debugging. It allows the user to collect and capture the pon, omci event logs.

Execute the following commands to set logging level and enable PON log debugging.

`#configure terminal`	Enter configure mode
`(config)#logging level pon 7`	Set logging level for PON messages
`(config)#exit`	Exit config mode
`#debug pon`	Enable PON debugging

Disable Logging and Debugging

Execute the following commands to disable PON log debugging.

```
#no debug pon
#show debugging pon

  PON State Machine debugging is OFF
  PON Task debugging is OFF
  PON OMCI debugging is ON
  PON NSM client debugging is OFF
```

CHAPTER 12 VLAN N:1 Configuration

Overview

For N:1 VLAN model, the ONT always adds the S-VLAN ID or translate an incoming tag to S-VLAN ID for upstream traffic. The OLT will pass-through any upstream traffic with S-VLAN ID on them. In the downstream direction, the OLT will pass-through traffic with S-VLAN ID to ONT by determining GEM Port based on MAC address and priority bits. If the GEM Port cannot be determined, then the frame is flooded using the unidirectional GEM Port associated with the S-VLAN ID. The ONT will remove the tag and forward frames from the GEM Port to appropriate U interface. For N:1 model, traffic is always single-tagged at V interface.

Topology

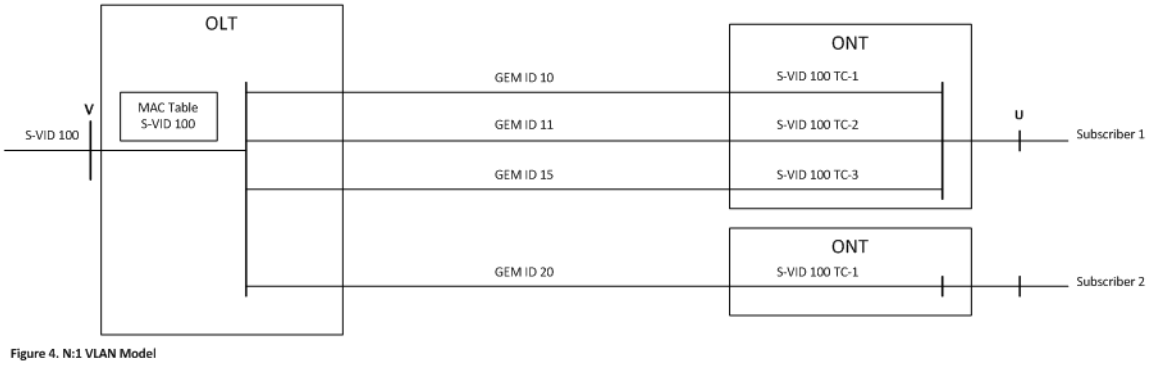


Figure 12-134: Subscriber Service Flow Configuration

VLAN n2one Flow Configuration

Configure ONU to add S-TAG or translate the incoming tag to right S-TAG for upstream traffic. OLT must program ONU such that S-VID should be removed/translated for the downstream traffic.

To configure S-VLAN flow for VLAN n2one, execute the following commands.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`(config-pon)# flow-id 0 mode n2one`	Input Flow identifier for mode n2one
`(config-pon-flow)#uni`	Enter UNI config flow mode
`(config-pon-flow-uni)#onu-id 0 uni-port-id 2 vlan-tag 101 translation-profile-name Untag_Sample ethertype 0x88a8`	Input ONU id, UNI port ID, vlan-tag, translation profile name for flow and ethertype should be 0x88a8 always for tibit
`(config-pon-flow-uni)#exit`	Exit PON flow UNI configuration mode
`(config-pon-flow)#nni`	Enter NNI config flow mode
`(config-pon-flow-nni)#olt-id 0 nni-port-name nni0/0/1 vlan-tag none`	Input OLT ID, NNI port name for flow

`(config-pon-flow-nni)#exit`	Exit configuration mode
`(config-pon-flow)#qos`	Enter QoS config flow mode
`(config-pon-flow-qos)#qos-profile-name QoS_Sample`	Input QoS Profile name
`(config-pon-flow-qos)#exit`	Exit configuration mode

Note: Ethertype field can be 0x8100 or 0x88a8 for UNI in case of AsxVolt16 but in tibit it should be always 0x88a8

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
#show pon flow brief

    FLOW-ID       FLOW-OPER-STATUS
    ------------------------------
    0             UP

OcNOS#sh pon flow 0
  flow-oper-status:     UP
  flow-mode:            n2one
  flow-statistics:      on
  ready-status:         READY
  pon-port:             pon0/0/1
  uni-end:
    onu-id:             0
    uni-port-id:        2
    trans-profile-name: Untag_Sample
    onu-vlan-tag:       101
    onu-tpid:           0x88a8
  nni-end:
    olt-id:             0
    nni-port-name:      nni0/0/1
    olt-vlan-tag:       0
  qos:
    qos-profile-name:   QoS_Sample
  tcont:
    T-CONT-NAME
    -----------
    tcont0
  gemport:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    GEM0                 2             0        0       0
```

CHAPTER 13 TC Layer Encryption Configuration

Overview

TC layer which is equivalent to Data Link layer of OSI model. It specifies GPON frame format, the media access control protocol, OAM processes and information encryption method. This TC layer encryption will do the encryption between OLT and ONU.

TC Layer Encryption Enable/Disable

Execute the following commands to enable or disable the TC layer encryption.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Configure PON parameters
`OcNOS(config-pon)# olt-id 0`	Input OLT Identifier
`OcNOS(config-pon-olt)#  serial-number 70:b3:d5:52:35:46`	Configure OLT serial number
`OcNOS(config-pon-olt)#  encryption on`	Enable the Encryption
`(config-pon-olt)# encryption off`	Disable the Encryption
`OcNOS(config-pon-olt)#  key-time 100`	Set the keytime on OLT
`(config-pon-olt)#exit`	Exit PON ONU configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Enable Encryption on Tibit

Change encryption on/off on Tibit platform requires pon port to be disabled. Disable PON port will affect ONU and flows.

Enable encryption before OLT configuration

```
OcNOS(config)#pon
OcNOS(config-pon)# olt-id 0
OcNOS(config-pon-olt)#  serial-number 70:b3:d5:52:35:46
OcNOS(config-pon-olt)#  encryption on
OcNOS(config-pon-olt)#  key-time 100
OcNOS(config-pon-olt)#  onu-provisioning-type automatic administrative-state up
```

Show command encryption stats before/after flow setup

```
OcNOS#show pon statistics pon-port pon0/0/1 onu 0 encryption

PON port = pon0/0/1 ONU_ID = 0
        encrypted_bytes  encrypted_pkts          plain_bytes      plain_pkts
-------------------------------------------------------------------------
```

```
TX                16224             338                    0               0
RX                    0               0                16512             344
Delete OLT and config without encryption

Check encryption stats before/after flow setup
OcNOS#show pon statistics pon-port pon0/0/1 onu 0 encryption

PON port = pon0/0/1 ONU_ID = 0
        encrypted_bytes  encrypted_pkts          plain_bytes      plain_pkts
-------------------------------------------------------------------------------
TX                    0               0                16176             337
RX                    0               0                16464             343
```

Enable Encryption on ASXvOLT-16

Enable encryption on ONU

```
OcNOS(config)#pon
OcNOS(config-pon)# onu-id 0
OcNOS(config-pon-onu)#  encryption on
OcNOS(config-pon-olt)#  key-time 100
```

Note: `show pon statistics` won't supported by ASXvOLT-16

CHAPTER 14 sFlow Configuration

Overview

sFlow is used for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization.

sFlow Enable/Disable

Execute the following commands to enable or disable the sFlow.

`#configure terminal`	Enter configure mode
`OcNOS(config)#feature sflow`	To Enable sFlow
`OcNOS(config)# sflow collector <ip-add> port <int> receiver-time-out 0`	To enable sFlow collector
`OcNOS(config)#interface pon0/0/1`	To Enter into PON port interface
`OcNOS(config-if)#sflow poll-interval <time-period>`	To Set the sFlow interval time
`OcNOS(config)#interface nni0/0/1`	To Enter into NNI interface
`OcNOS(config-if)#sflow poll-interval <time-period>`	To set the sFlow interval time
`OcNOS(config)#no feature sflow`	To Disable the sFlow
`OcNOS#show sflow brief`	This command will show the sFlow in brief
`OcNOS#show sflow detail`	This command will show the sFlow in detail
`OcNOS#show sflow interface pon0/0/1`	This will show the sFlow details on selected PON port
`OcNOS#show sflow interface nni0/0/1`	This will show the sFlow details on selected NNI interface
`OcNOS#show sflow statistics interface pon0/0/1`	This will show the sFlow statistics on selected PON onterface

Validation

This section shows the command(s) and output(s) to validate the configuration.

Enabling sFlow

```
OcNOS(config)#feature sflow
```

Adding sFlow collector

```
OcNOS(config)#sflow collector 172.29.1.99 port 6343 receiver-time-out 0 max-datagram-size 200
```

Enabling sFlow counter sampling on interface

```
OcNOS(config)#interface pon0/0/1
OcNOS(config-if)#sflow poll-interval 5
OcNOS(config-if)#exit
```

```
OcNOS(config)#interface nni0/0/1
OcNOS(config-if)#sflow poll-interval 5
```

Disabling the sFlow collector

```
OcNOS(config)#no sflow collector 172.29.1.99 port 6343 receiver-time-out 0 max-
datagram-size 200


#show sflow output
OcNOS#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 172.29.4.115
Collector IP: 0.0.0.0          Port:     0
Maximum Datagram Size(bytes): 0
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface      Counter-Polling
             Interval       Count
              (sec)
---------    --------------------
pon0/0/1            5          544
nni0/0/1            5          545
```

Execute the show command to verify the output.

Show sFlow

```
OcNOS#show sflow brief
sFlow Feature: Enabled
Collector IP: 172.29.1.99      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface      Counter-Polling
               Interval(secs)
---------      --------------------
pon0/0/1       5
nni0/0/1       5

OcNOS#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 172.29.4.115
Collector IP: 172.29.1.99      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0
 sFlow Port Detailed Information:
Interface      Counter-Polling
```

```
               Interval       Count
               (sec)
---------        --------------------
pon0/0/1           5          125
nni0/0/1           5          124

OcNOS#show sflow interface pon0/0/1
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 172.29.4.115
Collector IP: 172.29.1.99      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface      Counter-Polling
                 Interval       Count
                    (sec)
---------        --------------------
pon0/0/1             5          129


OcNOS#show sflow interface nni0/0/1
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 172.29.4.115
Collector IP: 172.29.1.99      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface      Counter-Polling
                      Interval       Count
                         (sec)
---------           --------------------
nni0/0/1                5          130


OcNOS#show sflow statistics interface pon0/0/1
 sFlow Port Statistics:
Interface  Counter-Polling
                            count
---------        ----------------
pon0/0/1           134

OcNOS#show sflow statistics interface nni0/0/1
 sFlow Port Statistics:
Interface  Counter-Polling
                          count
```

```
---------         ----------------
nni0/0/1            134
```

CHAPTER 15 Jumbo Frame Configuration

Overview

Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet MTU size. TIBIT supports jumbo frame MTU of size of 9000 bytes and alpha ONU supports MTU of size 8968 bytes.

To Configure Jumbo Frame Size

Execute the following commands to configure the jumbo frame size on UNI port.

`#configure terminal`	Enter configure mode
`(config)#pon-configuration`	Enter PON configure mode
`(config-pon)# onu-id 0`	Input ONU Identifier
`(config-pon-onu)#uni-port-id 0`	Input UNI port-ID
`OcNOS(config-pon-onu-uni)#mtu 6000`	Input the MTU for the UNI port
`(config-pon-olt)#exit`	Exit PON ONU configuration mode

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `config and show` command to verify the output.

```
OcNOS(config-pon-onu-uni)#mtu 6000
OcNOS#show pon onu 0
  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB8AF9(ALPHE3BB8AF9)
  onu-profile-name:  default_onu_profile
  admin-state:       UP
  oper-status:       UP
  encryption:        OFF
  uni-ports:         5
  tcont-maps:
    ALLOC-ID      TCONT-NAME            PON-PORT-NAME
    ------------------------------------------------
    1024          default_tcont         pon0/0/1
  gem-port-maps:
    GEM-PORT-ID   GEM-PORT-NAME         PON-PORT-NAME
    ------------------------------------------------
    1024          default_gemport       pon0/0/1
  onu-flow-list:
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   MAX-FRAME-SIZE   CONFIG-IND
    ------------------------------------------------------------------------
```

```
    0             UNLOCKED      ENABLED       6000            1G Ethernet full duplex

OcNOS(config-pon-onu-uni)#mtu 8986
OcNOS#show pon onu 0
  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB8AF9(ALPHE3BB8AF9)
  onu-profile-name:  default_onu_profile
  admin-state:       UP
  oper-status:       UP
  encryption:        OFF
  uni-ports:         5
  tcont-maps:
    ALLOC-ID      TCONT-NAME            PON-PORT-NAME
    ------------------------------------------------
    1024          default_tcont         pon0/0/1
  gem-port-maps:
    GEM-PORT-ID   GEM-PORT-NAME         PON-PORT-NAME
    ------------------------------------------------
    1024          default_gemport       pon0/0/1
  onu-flow-list:
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   MAX-FRAME-SIZE   CONFIG-IND
    ------------------------------------------------------------------------
    0             UNLOCKED      ENABLED       8986            1G Ethernet full duplex
```

CHAPTER 16 Rogue ONU detection and Isolation

Overview

A method of detecting a rogue ONU is an OLT detects an abnormal upstream traffic form the ONU to OLT. This will impact the other working ONUs which are connected on the OLT. The intention of this feature is to determine and isolate the rogue ONU from the OLT. This will help in smooth upstream transmission for the right ONUs.

Rogue ONU detection configuration

Execute the following commands to enable or disable the rogue ONU detection.

`#configure terminal`	Enter configure mode.
`(config)#pon-configuration`	Configure PON parameters.
`(config-pon)# onu-rogue-detection pon-port IFNAME`	Enabling rogue ONU detection for PON port.
`config-pon)# no onu-rogue-detection pon-port IFNAME`	Disabling rogue ONU detection for PON port.
`config-pon)# clear pon onu rogue onu serial-number <SERIAL_NUMER>`	To clear the rogue ONU data using ONU serial Number.
`(config-pon)# clear pon onu rogue pon-port <PON_PORT>`	To clear the rogue ONU data using pon-port-id.
`(config-pon)# onu isolate serial-number <SERIALNUMBER>  pon-port <IFNAME>)`	To isolate the rogue ONU using serial number or pon port.
`(config-pon)# no onu isolate serial-number <SERIALNUMBER>  pon-port <IFNAME>)`	To restore back the rogue ONU from isolate the rogue ONU using serial number or pon port.
`(OcNOS#show pon onu-rogue-detection pon-ports <WORD>`	This will show the rogue detection enabled state.
`(OcNOS)#show pon onu rogue`	This will show the suspected rogue ONUs.
`(OcNOS)#show pon onu isolated`	This will show the isolated rogue ONUs.
`(config-pon)#exit`	Exit configuration mode.

Validation

This section shows the command(s) and output(s) to validate the configuration.

To enable the rogue ONU configuration

```
OcNOS(config-pon)#onu-rogue-detection pon-port pon0/0/1
OcNOS(config-pon)#onu-rogue-detection pon-port pon0/0/2


OcNOS(config-pon)#
```

To isolate the rogue ONU

```
OcNOS(config-pon)# onu isolate serial-number 4252434D12345678 pon-port pon0/0/1
OcNOS(config-pon)#
```

To remove the ONU isolation

```
OcNOS(config-pon)#no onu isolate serial-number 4252434D12345678 pon-port pon0/0/1
```

Execute the show commands to verify the output.

```
OcNOS#sh pon olt 0
  admin-status:   UP
  oper-status:    UP
  onu-mode:       AUTOMATIC_PROVISION
  dhcp-mode:      OFF
  pon-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  ROGUE-DET
    ------------------------------------------------------------------
    pon0/0/1       UP            UP           -       XG-S   ON
OcNOS#show pon onu-rogue-detection pon-ports
  pon0/0/1
  pon0/0/2
OcNOS#
OcNOS#show pon onu rogue
  Serial Number(Vendor)   PON port        Count
  ---------------------------------------------
  -                       pon0/0/1        1

OcNOS#show pon onu isolated
  Serial Number(Vendor)   PON port
  ---------------------------------
  4252434D12345678(BRCM)  pon0/0/1
OcNOS#
```

CHAPTER 17 ONU Autofinding Configuration

Overview.

ONU Autofinding feature lists the serial numbers of ONU's which are unprovisioned.

Note: Works only in manual provisioning mode.

AsxVolt16:

```
OcNOS(config-pon)#olt-id 0
OcNOS(config-pon-olt)#onu-provisioning-type manual administrative-state up
```

TIBIT

`#configure terminal`	Enter configure mode.
`(config)#pon-configuration`	Enter PON configure mode.
`(config-pon)# olt-id 0`	Configure olt-Identifier.
`(config-pon-olt)# serial-number e8:b4:70:70:01:92`	Serial number for OLT.
`(config-pon-olt)# onu-provisioning-type manual administrative-state up`	Configure manual ONU provisioning type & Enable OLT admin state.
`(config-pon-olt)#exit`	Exit pon olt configure mode.
`#configure terminal`	Enter configure mode.

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

```
OcNOS#sh pon onu unprovisioned
  OLT-ID     PON-PORT     SERIAL#
  ------------------------------
  0          pon0/0/1     4246575300123130(BFWS00123130)
  0          pon0/0/1     414C5048E3BB8815(ALPHE3BB8815)
```

CHAPTER 18 Firmware Upgrade for Remote OLT (TIBIT)

Overview

OLT must provide a way to list down the firmware images on the four banks of TIBIT. User can copy the image to secondary bank than the active bank. Boot/reset the TIBIT MicroPlug from the specific bank after downloading the image.

To download firmware image and reboot follow the below commands.

`#configure terminal`	Enter configure mode.
`(config)#pon-configuration`	Configure PON parameters.
`(config-pon)# olt firmware-install olt-id 0 bank 0 file:///root/R1.3.0-OLT-FW.bin`	To download firmware image in bank 0.
`(config-pon)# olt reboot olt-id 0 bank 0`	To boot/reset the tibit microplug from specific bank.
`(config-pon-flow-acl)#exit`	Exit pon flow acl configure mode.

Validation

This section shows the command(s) and output(s) to validate the configuration.

Execute the `show` command to verify the output.

Check the existing firmware on the OLT

```
OcNOS# show pon olt 0 firmware-info
    BANK  |VERSION  |SHA      |DATE                      |ACTIVE  |NEXT-ACTIVE
    ------------------------------------------------------------------
    0     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |
    1     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |*       |*
    2     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |
    3     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |        |
```

After downloading the firmware image on bank 0

```
OcNOS#do show pon olt 0 firmware-info
    BANK  |VERSION  |SHA      |DATE                      |ACTIVE  |NEXT-ACTIVE
    ------------------------------------------------------------------
    0     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |        |*
    1     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |*       |
    2     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |
    3     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |        |
```

After reboot

```
OcNOS#show pon olt 0 firmware-info
    BANK  |VERSION  |SHA      |DATE                      |ACTIVE  |NEXT-ACTIVE
    ------------------------------------------------------------------
    0     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |*       |*
    1     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |
```

```
2     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |
3     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |        |
```

CHAPTER 19 FEC Enable/Disable Configuration

Overview

OLT enable downstream FEC per PON port by default. After Enabling upstream FEC OLT must be able to show the status of upstream FEC per ONU. To configure FEC execute the following commands. Edgecore platform will support enable/disable per ONU whereas TIBIT will keep the upstream FEC enabled by default.

FEC Enable/Disable

Execute the following commands to enable or disable the TC layer encryption.

`#configure terminal`	Enter configure mode.
`(config)#pon-configuration`	Configure PON parameters.
`OcNOS(config-pon)# onu-id <onu-id>`	Input ONU Identifier.
`OcNOS(config-pon-onu)# upstream-fec on`	To Enable the FEC.
`OcNOS(config-pon-onu)# upstream-fec off`	To Disable the FEC.
`OcNOS# show pon statistics onu <onu-id> fec`	To display the FEC statistics.

Validation

This section shows the command(s) and output(s) to validate the configuration.

Enable/Disable the FEC on ASXvOLT-16.

Enable the FEC

```
OcNOS(config)#pon
OcNOS(config-pon)# onu-id 2
OcNOS(config-pon-onu)#  upstream-fec on
```

Disable the FEC

```
OcNOS(config)#pon
OcNOS(config-pon)# onu-id 2
OcNOS(config-pon-onu)#  upstream-fec off
```

Show command for FEC statistics

```
OcNOS#sh pon statistics onu 2 fec

PON port = pon0/0/1 ONU_ID = 2
      codewords      corrected_bytes  codewords_corrected   uncorrectable
-------------------------------------------------------------------------
     1590347974                  816                 1202               2
OcNOS#
```

ONU Status when FEC is ON

```
OcNOS# show pon onu 2
  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB87DE(ALPHE3BB87DE)
  onu-profile-name:  onup1
  admin-state:       UP
  oper-status:       UP
  encryption:        OFF
  upstream-fec:      ON
  uni-ports:         5
```

Optical Line Termination Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Entering PON configuration Mode

This chapter contains commands for Entering PON configuration.

debug pon all

Use this command to enable debugging of PON module and OMCI stack.

Use the no parameter with this command to disable PON debugging.

Note: This enables POND and SM (State Machine).

Command Syntax

```
debug pon all
no debug pon all
```

Parameters

None

Default

By default, debug command is disabled.

Command Mode

PON configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS (config-pon) #debug pon all
```

pon-configuration

Use this command to enter the PON configuration mode.

Command Syntax

```
pon-configuration
```

Parameters

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS(config)#pon-configuration
OcNOS(config-pon)#
```

CHAPTER 2 Translation Profile Commands

This chapter contains commands for Translation Profile.

classification

Use this command to setup matching parameters for translation

Command Syntax

```
classification
```

Parameters

None

Default

None

Command Mode

PON TP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config-pon)#translation-profile profile-name tp1
(config-pon-tp)#classification
(config-pon-tp-classification)#vlan-type tagged vlan-id 3 p-bits 3
(config-pon-tp-classification)#exit
(config-pon-tp)#treatment
(config-pon-tp-treatment)#p-bits 3 operation remove-vlan
(config-pon-tp-treatment)#exit
(config-pon-tp)#exit
(config-pon)#no translation-profile profile-name tp1
(config-pon)#
```

p-bits

Use this command to indicate the translated p-bit and operation.

Command Syntax

```
p-bits <0-7> operation (none | remove-vlan)
```

Parameter

`<0-7>`	P-bits range
`none`	No action, only for vlan-type: untagged
`remove-vlan`	Remove matching VLAN, only for vlan-type:tagged/priorityTagged.

Command Mode

PON TP treatment mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config-pon)#translation-profile profile-name tp1
(config-pon-tp)#classification
(config-pon-tp-classification)#vlan-type tagged vlan-id 3 p-bits 3
(config-pon-tp-classification)#exit
(config-pon-tp)#treatment
(config-pon-tp-treatment)#p-bits 3 operation remove-vlan
(config-pon-tp-treatment)#exit
(config-pon-tp)#exit
(config-pon)#no translation-profile profile-name tp1
(config-pon)#
```

translation-profile

Use this command to setup the P-BIT & VLAN translation profile. Note that both tp-classification and tp-treatment must be set to complete tp configuration as illustrated in the example. However, they can be updated individually.

Use the no parameter to delete the translation profile with the specified profile name.

Command Syntax

```
translation-profile profile-name WORD
no translation-profile profile-name WORD
```

Parameter

`profile-name`	Indicate the `profile-name`
`WORD`	Translation Profile name

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config-pon)#translation-profile profile-name tp1
(config-pon-tp)#classification
(config-pon-tp-classification)#vlan-type tagged vlan-id 3 p-bits 3
(config-pon-tp-classification)#exit
(config-pon-tp)#treatment
(config-pon-tp-treatment)#p-bits 3 operation remove-vlan
(config-pon-tp-treatment)#exit
(config-pon-tp)#exit
(config-pon)#no translation-profile profile-name tp1
(config-pon)#
```

treatment

Use this command to setup the treatment parameters for translation.

Command Syntax

```
treatment
```

Parameter

None

Command Mode

PON TP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config-pon)#translation-profile profile-name tp1
(config-pon-tp)#classification
(config-pon-tp-classification)#vlan-type tagged vlan-id 3 p-bits 3
(config-pon-tp-classification)#exit
(config-pon-tp)#treatment
(config-pon-tp-treatment)#p-bits 3 operation remove-vlan
(config-pon-tp-treatment)#exit
(config-pon-tp)#exit
(config-pon)#no translation-profile profile-name tp1
(config-pon)#
```

vlan-type

Use this command to setup matching parameters for translation

Command Syntax

```
vlan-type untagged
vlan-type tagged vlan-id < 2-4094> p-bits <0-7>
Vlan-type prioritytagged p-bits <0-7>
```

Parameters

`vlan-id`	Indicate the VLAN Id to match as translation criteria
`<2-4094>`	VLAN Identifier range
`vlan-type`	Indicate the matching criteria for VLAN
`untagged`	Untagged VLAN, no vlan-id
`tagged`	Tagged VLAN, vlan-id is <2-4094>
`priority`	Tagged Priority tagged VLAN, vlan-id is 0
`p-bits`	Indicate the p-bits parameter
`<0-7>`	P-bits range

Default

None

Command Mode

PON TP classification mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config-pon)#translation-profile profile-name tp1
(config-pon-tp)#classification
(config-pon-tp-classification)#vlan-type tagged vlan-id 3 p-bits 3
(config-pon-tp-classification)#exit
(config-pon-tp)#treatment
(config-pon-tp-treatment)#p-bits 3 operation remove-vlan
(config-pon-tp-treatment)#exit
(config-pon-tp)#exit
(config-pon)#no translation-profile profile-name tp1
(config-pon)#
```

CHAPTER 3 QoS Profile Commands

This chapter contains commands for QoS Profile.

cir (PON QP Downstream mode)

Use this command to indicate CIR, PIR, and PBS parameters for downstream QoS Profile.

Command Syntax

```
cir <1-10000000> <kbps|mbps|gbps> pir <1-10000000> <kbps|mbps|gbps> pbs <1-
  10000000> <kbytes|mbytes|gbytes>
```

Parameter

None

Default

None

Command Mode

PON QP Downstream mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#pon-configuration
(config-pon)#qos-profile profile-name qp1
(config-pon-qp)#downstream
(config-pon-qp-downstream)#cir 1000 kbps pir 1200 kbps
(config-pon-qp-downstream)#exit
(config-pon-qp)#
```

cir (PON QP Upstream mode)

Use this command to indicate the CIR and PIR parameters for upstream QoS Profile.

Command Syntax

```
cir < 1-10000000 > <kbps|mbps|gbps> pir < 1-10000000> <kbps|mbps|gbps>
```

Parameters

None

Default

None

Command Mode

PON QP Upstream mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#qos-profile profile-name qp1
OcNOS(config-pon-qp)#upstream
OcNOS(config-pon-qp-upstream)#cir 1000 kbps pir 1200 kbps
OcNOS(config-pon-qp-upstream)#exit
OcNOS(config-pon-qp)#
```

downstream

Use this command to setup the downstream parameters for QoS Profile.

Note: Refer the following:

- It is recommended to set the value of cir/pir to ~4%-5% more than desired rate limit to account for the Inter packet gap.
- TIBIT OLT support range of 272Kbytes-1256Kbytes for PBS.

```
OcNOS(config-pon-qp-downstream)#cir ?
<1-10000000> Downstream Committed information rate 1kbps- 10gbps.Set the
value to ~4%-5% more than desired rate limit to account for inter packet gap
OcNOS(config-pon-qp-downstream)#cir 1 kbps pir ?
<1-10000000> Downstream Committed information rate 1kbps- 10gbps.Set the
value to ~4%-5% more than desired rate limit to account for inter packet gap
OcNOS(config-pon-qp-downstream)#cir 1 kbps pir 256 kbps pbs ?
<1-10000000>  Downstream PBS 1Kbytes-10Gbytes
```

Command Syntax

```
downstream
```

Parameter

None

Default

None

Command Mode

PON QP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#qos-profile profile-name qp1
OcNOS(config-pon-qp)#downstream
OcNOS(config-pon-qp-downstream)#cir 1000 kbps pir 1200 kbps pbs 1200 kbytes
OcNOS(config-pon-qp-downstream)#exit
OcNOS(config-pon-qp)#
```

qos-profile

Use this command to setup the QoS profile parameters. Note that both qp-upstream & qp-downstream must be set to complete tp configuration as illustrated in the example. However, they can be updated individually.

Use the no parameter to delete the QoS profile with the specified profile name.

Command Syntax

```
qos-profile profile-name WORD
no qos-profile profile-name WORD
```

Parameter

WORD	Input QoS Profile name

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#qos-profile profile-name qp1
OcNOS(config-pon-qp)#downstream
OcNOS(config-pon-qp-downstream)#cir 15 mbps pir 20 mbps pbs 30 mbytes
OcNOS(config-pon-qp-downstream)#exit
OcNOS(config-pon-qp)#upstream
OcNOS(config-pon-qp-upstream)#cir 15 mbps pir 20 mbps
OcNOS(config-pon-qp-upstream)#exit
OcNOS(config-pon-qp)#exit

OcNOS(config-pon)#no qos-profile profile-name qp1
OcNOS(config-pon)#
```

upstream

Use this command to setup the upstream parameters for QoS Profile.

Note: Refer the following:

- CIR/PIR will be rounded to the nearest multiple of 128kbps.
- PIR should be GREATER than CIR by at least 128kbps.

```
OcNOS(config-pon-qp-upstream)#cir 1 kbps pir ?
 <1-10000000> Upstream Peak information rate 1kbps-10Gbps. Should be at
 least 128Kbps more than CIR. Will be rounded to the nearest
 multiple of 128Kbps

 <kbps|mbps|gbps>
  gbps  Specifies the units of gigabits per second
  kbps  Specifies the units of kilobits per second
  mbps  Specifies the units of megabits per second
```

Command Syntax

```
upstream
```

Parameters

None

Default

None

Command Mode

PON QP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#qos-profile profile-name qp1
OcNOS(config-pon-qp)#upstream
OcNOS(config-pon-qp-upstream)#cir 1000 kbps pir 1200 kbps
OcNOS(config-pon-qp-upstream)#exit
OcNOS(config-pon-qp)#
```

CHAPTER 4 ONU Profile Commands

This chapter contains commands for ONU Profile.

gem-port-name (PON OP TCONT mode)

Use this command to setup the gem port name.

Note: Associate only one GEM-Port to one T-Cont for TIBIT OLT.

Command Syntax

```
gem-port-name WORD
```

Parameter

WORD	Input tcont name

Default

None

Command Mode

PON OP TCONT mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#pon-configuration
(config-pon)#onu-profile profile-name op1
(config-pon-op)#uni port-id 1
(config-pon-op-uni)#gem-port-name GEM1 p-bits 1 upstream-priority-queue 1
downstream-priority-queue 2
(config-pon-op-uni)#gem-port-name GEM2 p-bits 2 upstream-priority-queue 3
downstream-priority-queue 4
(config-pon-op-uni)#gem-port-name GEM3 p-bits 3 upstream-priority-queue 5
downstream-priority-queue 6
(config-pon-op-uni)#exit
(config-pon-op)#uni port-id 2
(config-pon-op-uni)#gem-port-name GEM4 p-bits 4 upstream-priority-queue 7
downstream-priority-queue 8
(config-pon-op-uni)#gem-port-name GEM5 p-bits 5 upstream-priority-queue 9
downstream-priority-queue 10
(config-pon-op-uni)#gem-port-name GEM6 p-bits 6 upstream-priority-queue 11
downstream-priority-queue 12
(config-pon-op-uni)#exit
(config-pon-op)#t-cont tc1
(config-pon-op-t-cont)#gem-port-name GEM1
(config-pon-op-t-cont)#gem-port-name GEM4
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc2
(config-pon-op-t-cont)#gem-port-name GEM2
(config-pon-op-t-cont)#gem-port-name GEM5
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc3
(config-pon-op-t-cont)#gem-port-name GEM3
(config-pon-op-t-cont)#gem-port-name GEM6
```

```
(config-pon-op-t-cont)#exit
```

gem-port-name (PON OP UNI mode)

Use this command to setup GEM port name.

Command Syntax

```
gem-port-name WORD
```

Parameters

WORD	Indicate the gem port name

Default

None

Command Mode

PON OP UNI mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#pon-configuration
(config-pon)#onu-profile profile-name op1
(config-pon-op)#uni port-id 1
(config-pon-op-uni)#gem-port-name GEM1 p-bits 1 upstream-priority-queue 1
downstream-priority-queue 2
(config-pon-op-uni)#gem-port-name GEM2 p-bits 2 upstream-priority-queue 3
downstream-priority-queue 4
(config-pon-op-uni)#gem-port-name GEM3 p-bits 3 upstream-priority-queue 5
downstream-priority-queue 6
(config-pon-op-uni)#exit
(config-pon-op)#uni port-id 2
(config-pon-op-uni)#gem-port-name GEM4 p-bits 4 upstream-priority-queue 7
downstream-priority-queue 8
(config-pon-op-uni)#gem-port-name GEM5 p-bits 5 upstream-priority-queue 9
downstream-priority-queue 10
(config-pon-op-uni)#gem-port-name GEM6 p-bits 6 upstream-priority-queue 11
downstream-priority-queue 12
(config-pon-op-uni)#exit
(config-pon-op)#t-cont tc1
(config-pon-op-t-cont)#gem-port-name GEM1
(config-pon-op-t-cont)#gem-port-name GEM4
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc2
(config-pon-op-t-cont)#gem-port-name GEM2
(config-pon-op-t-cont)#gem-port-name GEM5
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc3
(config-pon-op-t-cont)#gem-port-name GEM3
(config-pon-op-t-cont)#gem-port-name GEM6
(config-pon-op-t-cont)#exit
```

onu-profile

Use this command to setup the ONU profile parameters. Note that op-uni for all uni ports & op-tcont for all tcont identifiers must be set to complete op configurations as illustrated in the example. However, uni & tcont rules can be updated individually.

Use the no parameter to delete the ONU profile with the specified profile name, delete uni port with specified port id or delete t-cont with specified name.

Command Syntax

```
onu-profile profile-name WORD
no onu-profile profile-name WORD
```

Parameter

WORD	Input QoS Profile name

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#pon-configuration
(config-pon)#onu-profile profile-name op1
(config-pon-op)#uni port-id 1
(config-pon-op-uni)#gem-port-name GEM1 p-bits 1 upstream-priority-queue 1
downstream-priority-queue 2
(config-pon-op-uni)#gem-port-name GEM2 p-bits 2 upstream-priority-queue 3
downstream-priority-queue 4
(config-pon-op-uni)#gem-port-name GEM3 p-bits 3 upstream-priority-queue 5
downstream-priority-queue 6
(config-pon-op-uni)#exit
(config-pon-op)#uni port-id 2
(config-pon-op-uni)#gem-port-name GEM4 p-bits 4 upstream-priority-queue 7
downstream-priority-queue 8
(config-pon-op-uni)#gem-port-name GEM5 p-bits 5 upstream-priority-queue 9
downstream-priority-queue 10
(config-pon-op-uni)#gem-port-name GEM6 p-bits 6 upstream-priority-queue 11
downstream-priority-queue 12
(config-pon-op-uni)#exit
(config-pon-op)#t-cont tc1
(config-pon-op-t-cont)#gem-port-name GEM1
(config-pon-op-t-cont)#gem-port-name GEM4
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc2
(config-pon-op-t-cont)#gem-port-name GEM2
(config-pon-op-t-cont)#gem-port-name GEM5
```

```
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc3
(config-pon-op-t-cont)#gem-port-name GEM3
(config-pon-op-t-cont)#gem-port-name GEM6
(config-pon-op-t-cont)#exit
```

t-cont

Use this command to setup T-Cont port to GEM port connections for ONU Profile.

Command Syntax

```
tcont WORD
```

Parameter

WORD	Input tcont name

Default

None

Command Mode

PON OP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#pon-configuration
(config-pon)#onu-profile profile-name op1
(config-pon-op)#uni port-id 1
(config-pon-op-uni)#gem-port-name GEM1 p-bits 1 upstream-priority-queue 1
downstream-priority-queue 2
(config-pon-op-uni)#gem-port-name GEM2 p-bits 2 upstream-priority-queue 3
downstream-priority-queue 4
(config-pon-op-uni)#gem-port-name GEM3 p-bits 3 upstream-priority-queue 5
downstream-priority-queue 6
(config-pon-op-uni)#exit
(config-pon-op)#uni port-id 2
(config-pon-op-uni)#gem-port-name GEM4 p-bits 4 upstream-priority-queue 7
downstream-priority-queue 8
(config-pon-op-uni)#gem-port-name GEM5 p-bits 5 upstream-priority-queue 9
downstream-priority-queue 10
(config-pon-op-uni)#gem-port-name GEM6 p-bits 6 upstream-priority-queue 11
downstream-priority-queue 12
(config-pon-op-uni)#exit
(config-pon-op)#t-cont tc1
(config-pon-op-t-cont)#gem-port-name GEM1
(config-pon-op-t-cont)#gem-port-name GEM4
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc2
(config-pon-op-t-cont)#gem-port-name GEM2
(config-pon-op-t-cont)#gem-port-name GEM5
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc3
(config-pon-op-t-cont)#gem-port-name GEM3
(config-pon-op-t-cont)#gem-port-name GEM6
(config-pon-op-t-cont)#exit
```

uni port-id

Use this command to setup UNI port to GEM port connections for ONU Profile.

Command Syntax

```
uni port-id <0-255>
```

Parameters

port-id	Indicate the port id

Default

None

Command Mode

PON OP mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#pon-configuration
(config-pon)#onu-profile profile-name op1
(config-pon-op)#uni port-id 1
(config-pon-op-uni)#gem-port-name GEM1 p-bits 1 upstream-priority-queue 1
downstream-priority-queue 2
(config-pon-op-uni)#gem-port-name GEM2 p-bits 2 upstream-priority-queue 3
downstream-priority-queue 4
(config-pon-op-uni)#gem-port-name GEM3 p-bits 3 upstream-priority-queue 5
downstream-priority-queue 6
(config-pon-op-uni)#exit
(config-pon-op)#uni port-id 2
(config-pon-op-uni)#gem-port-name GEM4 p-bits 4 upstream-priority-queue 7
downstream-priority-queue 8
(config-pon-op-uni)#gem-port-name GEM5 p-bits 5 upstream-priority-queue 9
downstream-priority-queue 10
(config-pon-op-uni)#gem-port-name GEM6 p-bits 6 upstream-priority-queue 11
downstream-priority-queue 12
(config-pon-op-uni)#exit
(config-pon-op)#t-cont tc1
(config-pon-op-t-cont)#gem-port-name GEM1
(config-pon-op-t-cont)#gem-port-name GEM4
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc2
(config-pon-op-t-cont)#gem-port-name GEM2
(config-pon-op-t-cont)#gem-port-name GEM5
(config-pon-op-t-cont)#exit
(config-pon-op)#t-cont tc3
(config-pon-op-t-cont)#gem-port-name GEM3
(config-pon-op-t-cont)#gem-port-name GEM6
(config-pon-op-t-cont)#exit
```

CHAPTER 5 OLT Commands

This chapter contains commands for OLT.

dhcp

Use this command to setup the DHCP relay Option 82 parameter.

Command Syntax

```
dhcp (off | on)
```

Parameter

off	No DHCP relay Option 82 processing
on	DHCP relay Option 82 processing

Default

None

Command Mode

PON OLT mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#pon-configuration
(config-pon)#olt-id 1
(config-pon-olt)#onu-provisioning-type manual administrative-state up
(config-pon-olt)#dhcp on
(config-pon-olt)# exit
(config-pon)
```

encryption

Use this command to change encryption state on/off.

Note: Encryption state can be changed on OLT cli level on TIBIT VM.

Command Syntax

```
encryption(on|off)
```

Parameter

off	The encryption is disabled
on	The encryption is enabled

Default

Encryption state is disabled by default.

Command Mode

PON OLT mode on TIBIT VM, and PON ONU on ASXvOLT16

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#config terminal
(config)#pon
(config-pon)#olt-id 30
(config-pon-olt)#serial-number e8b47070013e
(config-pon-olt)#encryption on
(config-pon-olt)#onu-provisioning-type automatic administrative-state up
(config-pon-olt)#end
```

key-time

Use this command to change a key exchange interval.

Note: The change can happen before and after the OLT configuration. 'show running-config' shall reflect the new value.

Command Syntax

```
key-time <10-3600>   - ASXvOLT16
key-time <60-3600>   - Tibit
```

Parameter

<10-3600>	Number of seconds (ASXvOLT16)
<60-3600>	Number of seconds (Tibit)

Default

Default key-time value is 60 and will not show in 'show running-config'.

Command Mode

PON OLT mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#config terminal
(config)#pon
(config-pon)#olt-id 30
(config-pon-olt)#serial-number e8b47070013e
(config-pon-olt)#key-time 100
(config-pon-olt)#onu-provisioning-type automatic administrative-state up
(config-pon-olt)#end
```

olt firmware-install

Use this command to install firmware on TIBIT microplug.

User can specify which bank to install the firmware with this command, TIBIT microplug can hold up to four different firmwares in its banks. A new firmware can not be installed on Active or Next Active bank. On successful installation, the next active bank is set to the newly installed firmware bank. For microplug to boot from Next Active bank requires a reboot of OLT.

Command Syntax

```
olt firmware-install olt-id <0-63> bank <0-3> URL
```

Parameter

<0-63>	Olt on which firmware will be installed
<0-3>	Olt bank on which firmware will be installed. Cannot be Active or Next Active bank
URL	A file system path where to get firmware binary. file://mnt/usb/path/to/file/<firmware.bin>

Default

None

Command Mode

PON OLT mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#configure pon terminal
OcNOS(config-pon)#do show pon olt 0 firmware-info
    BANK  |VERSION  |SHA      |DATE                     |ACTIVE  |NEXT-ACTIVE
    ------------------------------------------------------------------
    0     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |*       |*
    1     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |        |
    2     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |        |
    3     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |        |
OcNOS(config-pon)#olt firmware-install olt-id 0 bank 1 file:///home/ocnos/
R1.2.0-OLT-FW.bin
OcNOS(config-pon)#do show pon olt 0 firmware-info
    BANK  |VERSION  |SHA      |DATE                     |ACTIVE  |NEXT-ACTIVE
    ------------------------------------------------------------------
    0     |R1.3.0   |de6b297  |Thu May 28 23:53:59 2020 |*       |
    1     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40 2020 |        |*
    2     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |        |
    3     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |        |
OcNOS(config-pon)#olt reboot olt-id 0
OcNOS(config-pon)#do show pon olt 0 firmware-info     BANK  |VERSION  |SHA
|DATE                     |ACTIVE  |NEXT-ACTIVE     -------------------------
-------------------------------------     0     |R1.3.0   |de6b297  |Thu May
28 23:53:59 2020 |        |     1     |R1.2.0   |3cba51d  |Fri Feb 28 00:18:40
```

```
2020 |*       |*     2     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |
|      3     |R1.2.1   |fa23467  |Fri Mar  6 22:03:25 2020 |         |
```

olt-id

Use this command to setup the OLT parameters like ONU Provisioning type, OLT Administrative State and DHCP Relay Option 82 state.

Note: Supports single OLT for ASXvOLT16 and the TIBIT OLT supports 0-63 range for OLT-ID.

Use no prefix to delete OLT on TIBIT OLT only.

Command Syntax

```
olt-id <0-65535>
no olt-id <0-63>
```

Parameter

<0-65535>	Input OLT identifier value (For future use)
<0-63>	Input OLT identifier for TIBIT OLT

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#pon-configuration
(config-pon)#olt-id 1
(config-pon-olt)#onu-provisioning-type manual administrative-state up
(config-pon-olt)#dhcp on
(config-pon-olt)# exit
(config-pon)
```

olt reboot

Use this command to reboot a specific OLT in TIBIT VM. If no bank is specified, microplug boots with Next Active bank.

Command Syntax

```
olt reboot olt-id <0-63> (bank <0-3>)
```

Parameter

<0-63>	Input OLT identifier value
<0-3>	Input bank value

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.1 and changed in OcNOS-SP version 4.0.

Example

```
#configure terminal
(config)#pon-configuration
(config-pon-olt)# olt reboot olt-id 0

Reboot OLT with firmware in bank 1:
#configure terminal
(config)#pon-configuration
(config-pon-olt)# olt reboot olt-id 0 bank 1
```

onu-provisioning-type

Use this command to setup the ONU Provisioning type parameter.

Note: ONU provisioning mode can be changed dynamically from automatic to manual or from manual to automatic only on TIBIT OLT.

Command Syntax

```
onu-provisioning-type (manual|automatic)administrative-state (disable|enable)
```

Parameter

`manual`	All ONUs connecting to OLT are manual provisioned
`automatic`	All ONUs connecting to OLT are automatic provisioned
`disable`	The OLT is disabled
`enable`	Input OLT is enabed

Default

None

Command Mode

PON OLT mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#configure terminal
(config)#pon-configuration
(config-pon)#olt-id 1
(config-pon-olt)#onu-provisioning-type manual administrative-state up
(config-pon-olt)#dhcp on
(config-pon-olt)# exit
(config-pon)
```

CHAPTER 6 ONU Commands

This chapter contains commands for ONU.

administrative-state

Use this command to lock or unlock the UNI port.

Command Syntax

```
administrative-state <lock | unlock>
```

Parameter

`lock`	To lock UNI port
`unlock`	To unlock UNI port

Default

None

Command Mode

PON ONU UNI mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)#olt olt-id 1 port-name pon0/0/1 serial-number
ABCD12AC34BC
onu-profile-name op1
OcNOS(config-pon-onu)#uni-port-id 1
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#uni-port-id 2
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#exit
OcNOS(config-pon)#no onu-id 1
```

clear pon onu rogue

Use this command to clear Rogue suspect data for an ONU or PON port.

Command Syntax

```
clear pon onu rogue onu serial-number WORD
clear pon onu rogue pon-port WORD
```

Parameter

WORD	Input Serial number identifier value
WORD	Input pon port value

Default

None

Command Mode

EXEC Mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
OcNOS#clear pon onu rogue onu serial-number ABCD12345678
OcNOS#clear pon onu rogue pon-port pon0/0/1
```

disable/enable

Use this command to disable or enable the ONU.

Command Syntax

```
disable
enable
```

Parameters

`disable`	Disable the ONU
`enable`	Enable the ONU

Default

None

Command Mode

PON ONU mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)disable
OcNOS(config-pon-onu)enable
```

encryption

Use this command to enable/disable TC layer encryption on ASXvOLT16.

Command Syntax

```
encryption <on/off>
```

Parameters

on	Encryption ON
off	Encryption OFF

Default

Encryption is disabled by default.

Command Mode

PON ONU mode on ASXvOLT16.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#config terminal
(config)#pon
(config-pon)#olt-id 30
(config-pon-olt)#onu-provisioning-type automatic administrative-state up
(config-pon-olt)#onu-id 0
(config-pon-onu)#encryption on
```

mtu

Use this command to set maximum packet size value for the UNI port.

Command Syntax

```
mtu <576-8986>
```

Parameters

<576-8986>	MTU range

Default

The default value is 1518.

Command Mode

PON ONU mode on ASXvOLT16.

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)#olt olt-id 1 port-name pon0/0/1 serial-number
ABCD12AC34BC
onu-profile-name op1
OcNOS(config-pon-onu)#uni-port-id 1
OcNOS(config-pon-onu-uni)#mtu 6000
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#exit
OcNOS(config-pon)#no onu-id 1
```

olt olt-id

Use this command to setup the ONU identifier parameter.

Command Syntax

```
olt olt-id <0-65535> pon-port WORD serial-number WORD onu-profile-name WORD
```

Parameter

<0-65535>	Input ONU identifier value
WORD	Input pon port value
WORD	Input serial number identifier value
WORD	Input ONU profile name value

Default

None

Command Mode

PON ONU mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)#olt olt-id 1 port-name pon0/0/1 serial-number
ABCD12AC34BC
onu-profile-name op1
OcNOS(config-pon-onu)#uni-port-id 1
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#uni-port-id 2
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#exit
OcNOS(config-pon)#no onu-id 1
OcNOS(config-pon)#
```

onu isolate

Use this command to isolate ONU.

Use the no form of this command to de-isolate ONU.

Command Syntax

```
onu isolate serial-number WORD (pon-port WORD |)
```

Parameter

WORD	Input Serial number identifier value
WORD	Input PON port value

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
OcNOS(config-pon)#onu isolate serial-number ABCD12345678 pon-port pon0/0/1
OcNOS(config-pon)#no onu isolate serial-number ABCD12345678
```

onu mibreset

Use this command to launch mibreset for the ONU.

Command Syntax

```
onu mibreset onu-id <0-4095>
```

Parameter

`<0-4095>`	Input ONU identifier value for mibreset

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS(config-pon)#onu mibreset onu-id 0
```

onu reboot

Use this command to reboot the ONU.

Command Syntax

```
onu reboot onu-id <0-4095>
```

Parameter

<0-4095>	Input ONU identifier value to reboot

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS(config-pon)#onu reboot onu-id 0
```

onu-id

Use this command to setup the ONU. It includes parameters to specify the connected OLT, the connected PON port, serial number of ONU and translation profile associated with the ONU. The UNI submenu is to configure each UNI port of the ONU.

Use the no parameter to delete ONU with specific ONU Identifier.

Command Syntax

```
onu-id <0-4095>
no onu-id <0-4095>
```

Parameter

<0-4095>	Input ONU identifier value

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)#olt olt-id 1 port-name pon0/0/1 serial-number
ABCD12AC34BC onu-profile-name op1
OcNOS(config-pon-onu)#uni-port-id 1
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#uni-port-id 2
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#exit
OcNOS(config-pon)#no onu-id 1
OcNOS(config-pon)#
```

onu-profile-name

Use this command to change the ONU profile name associated with the ONU.

Command Syntax

```
onu-profile-name WORD force-delete-flows <yes | no>
```

Parameter

WORD	Input ONU profile name
yes	Delete dependent flows
no	Do not delete dependent flows

Default

None

Command Mode

PON ONU mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS(config-pon)#onu-id 1
OcNOS(config-pon-onu)#onu-profile-name op1 force-delete-flows yes
```

uni-port-id

Use this command to setup the UNI ports for ONU.

Command Syntax

```
uni-port-id <0-255>
```

Parameter

<0-255>	Input UNI identifier value

Default

None

Command Mode

PON ONU mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#onu-id 1
OcNOS(onu)#olt olt-id 1 port-name pon0/0/1 serial-number ABCD12AC34BC
onu-profile-name op1
OcNOS(config-pon-onu)#uni-port-id 1
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#uni-port-id 2
OcNOS(config-pon-onu-uni)#administrative-state unlock
OcNOS(config-pon-onu-uni)#exit
OcNOS(config-pon-onu)#exit
OcNOS(config-pon)#no onu-id 1
OcNOS(config-pon)#
```

upstream-fec

Use this command to change upstream-fec on ASXvOLT16.

Command Syntax

```
upstream-fec <on/off>
```

Parameter

on	FEC ON
off	FEC OFF

Default

FEC is enabled by default.

Command Mode

PON ONU mode on ASXvOLT16

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#config terminal
(config)#pon
(config-pon)#olt-id 30
(config-pon-olt)#onu-provisioning-type automatic administrative-state up
(config-pon-olt)#onu-id 0
(config-pon-onu)#upstream-fec off
```

CHAPTER 7 Flow Commands

This chapter contains commands for Flow:

dump acl trap

Use this command to dump trapped packets to the file of /tmp/pon_acl_trap_dump.pcap.

Command Syntax

```
dump acl trap enable (flow-id <0-65535> |) (acl-id <0-65535> |) (direction
  (upstream|downstream) |) (limit <1-4000>|)
```

Parameter

`dump acl trap enable`	Command to dump ACL trap enable
`flow-id`	Flow identifier to dump
`<0-65535>`	Flow identifier value
`acl-id`	ACL rule identifier
`<0-65535>`	Input ACL rule identifier value
`direction`	Indicate direction to apply ACL rule
`upstream`	ACL rule to be applied in upstream direction
`downstream`	ACL rule to be applied in downstream direction
`limit`	Size in MB of packet data to trap for matching rule
`<1-4000>`	Input size in MB of packet data to dump value

Default

flow-id: any flow that has trap ACLs if not set

acl-id: any PON trap ACL rule if not set

Direction: both downstream and upstream directions if not set

Limit: 10MB if not set (1MB = 1024 * 1024)

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#dump acl trap enable
OcNOS(config-pon)#exit
OcNOS(config)#

OcNOS(config-pon)#no dump acl trap enable

OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#dump acl trap enable flow-id 1 direction upstream limit 4
OcNOS(config-pon)#exit
```

```
OcNOS(config)#

OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#dump acl trap enable flow-id 1 acl-id 1 limit 4
OcNOS(config-pon)#exit
OcNOS(config)#
```

flow-id

Use this command to setup the Subscriber Service flows. It consists of UNI, NNI, QoS and ACL submenus.

Use the no parameter to delete the Flow with the specified flow identifier.

Command Syntax

```
flow-id <0-65535>(mode n2one/one2one)
no flow-id <0-65535>
```

Parameter

<0-65535>	Input Flow identifier value
n2one/one2one	Specifies mode of the flow (default mode is one2one)

Default

None

Command Mode

PON Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#uni
OcNOS(config-pon-flow-uni)#onu-id 0 uni-port-id 0 vlan-tag 20 translation-
profile-name tp1
OcNOS(config-pon-flow-uni)#exit
OcNOS(config-pon-flow)#nni
OcNOS(config-pon-flow-nni)#olt-id 1 nni-port-name nni0/0/1 vlan-tag 1
OcNOS(config-pon-flow-nni)#exit
OcNOS(config-pon-flow)#qos
OcNOS(config-pon-flow-qos)#qos-profile-name qp1
OcNOS(config-pon-flow-qos)#exit
OcNOS(config-pon-flow)# exit
OcNOS(config-pon)#no flow-id 1
OcNOS(config-pon)#
```

nni

Use this command to setup NNI parameters of flow. ‘vlan-tag’ is optional parameter.

Command Syntax

```
nni
```

Parameter

None

Default

None

Command Mode

PON Flow mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#nni
OcNOS(config-pon-flow-nni)#olt-id 1 nni-port-name nni0/0/1 vlan-tag 1
OcNOS(config-pon-flow-nni)#exit
```

olt-id

Use this command to setup OLT identifier, NNI port name, VLAN tag type and VLAN tag for NNI leg of flow.

Command Syntax

```
olt-id <0-65535> nni-port-name WORD vlan-tag <2-4094>/none (ethertype 0x8100/
  0x88a8)
```

Parameter

`<0-65535>`	Input OLT identifier value for Flow
`WORD`	Input NNI port identifier value for Flow
`<2-4094>`	Input vlan tag identifier for NNI leg of Flow
`0x8100/0x88a8`	Tag Protocol ID for VLAN tag

Default

None

Command Mode

PON Flow NNI mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#nni
OcNOS(config-pon-flow-nni)#olt-id 1 nni-port-name nni0/0/1 vlan-tag none
OcNOS(config-pon-flow-nni)#exit
```

onu-id

Use this command to setup the ONU identifier, UNI port identifier, translation profile name, vlan tag type and vlan tag for UNI leg of the flow.

Command Syntax

```
onu-id <0-4095> uni-port-id <0-255> vlan-tag <2-4094> translation-profile-name
  WORD (ethertype 0x88a8)
```

Parameter

`<0-4095>`	Input ONU identifier value for Flow
`<0-255>`	Input uni port identifier value for Flow
`<2-4094>`	Input vlan tag identifier for UNI leg of Flow
`WORD`	Input translation profile name for UNI leg of Flow
`0x88a8`	Replace ETHERTYPE to 0x88a8 for flow

Default

None

Command Mode

PON Flow UNI mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#uni
OcNOS(config-pon-flow-uni)#onu-id 1 uni-port-id 1 vlan-tag 3 translation-
profile-name tp1 ethertype 0x88a8
OcNOS(config-pon-flow-uni)#exit
OcNOS(config-pon-flow)#nni
OcNOS(config-pon-flow-nni)#olt-id 1 nni-port-name nni0/0/1 vlan-tag 1
OcNOS(config-pon-flow-nni)#exit
OcNOS(config-pon-flow)#qos
OcNOS(config-pon-flow-qos)#qos-profile-name qp1
OcNOS(config-pon-flow-qos)#exit
OcNOS(config-pon-flow)# exit
OcNOS(config-pon)#no flow-id 1
OcNOS(config-pon)#
```

pon-acl-id

Use this command to setup ACL rules of a subscriber service flow.

Note: The Applicable rule must have priority, action and direction.

Command Syntax

```
pon-acl-id <0-65535> (priority <0-65535>|) (action (allow|drop|trap-to-cpu)|)
  (direction (upstream|downstream)|) (remote-ip (A.B.C.D|X:X::X:X) |) (protocol
  (tcp|udp|any)|) (remote-port <1-65535>|)
```

Parameter

`pon-acl-id`	ACL rule identifier (mandatory)
`<0-65535>`	Input ACL rule identifier value
`priority`	Priority of ACL rule
`<0-65535>`	Input priority value
`action`	Action for packet matching ACL rule
`allow`	Allow matching packets
`drop`	Drop matching packets
`trap-to-cpu`	Trap matching packets to CPU
`direction`	Indicate direction to apply ACL rule
`upstream`	ACL rule to be applied in upstream direction
`downstream`	ACL rule to be applied in downstream direction
`remote-ip`	Downstream source/Upstream destination IP for ACL
`A.B.C.D`	IPv4 address for ACL rule
`X:X::X:X`	IPv6 format for ACL rule
`protocol`	Indicate protocol for ACL rule
`udp`	Apply rule for UDP matching packets
`tcp`	Apply rule for TCP matching packets
`any`	Apply rule for any matching packets
`remote-port`	Downstream source/Upstream destination port for ACL
`<1-65535>`	Value for port

Default

Value not set

Command Mode

PON Flow mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#acl
OcNOS(config-pon-flow-acl)# pon-acl-id 1 priority 10 action drop direction
upstream remote-ip 1.2.3.4 protocol tcp remote-port 123
OcNOS(config-pon-flow-acl)# pon-acl-id 2 priority 20 action drop direction
upstream remote-ip 1.2.3.4 protocol udp
OcNOS(config-pon-flow-acl)# pon-acl-id 3 priority 30 action trap-to-cpu
direction upstream remote-ip 1.2.3.5
OcNOS(config-pon-flow-acl)# pon-acl-id 4 priority 29 action allow direction
upstream remote-ip 1.2.3.5 remote-port 123
OcNOS(config-pon-flow-acl)# pon-acl-id 5
OcNOS(config-pon-flow-acl)#no pon-acl-id 1
OcNOS(config-pon-flow-acl)#exit
OcNOS(config-pon-flow)#no acl
OcNOS(config-pon-flow)#
```

qos

Use this command to set the qos profile for the flow.

Command Syntax

```
qos
```

Parameter

None

Default

None

Command Mode

PON Flow mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#qos
OcNOS(config-pon-flow-qos)#qos-profile-name qp1
OcNOS(config-pon-flow-qos)#exit
```

qos-profile-name

Use this command to set the qos profile name parameter for the flow.

Command Syntax

```
qos-profile-name WORD
```

Parameter

WORD	Input QOS profile name

Default

None

Command Mode

PON Flow QOS mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#qos
OcNOS(config-pon-flow-qos)#qos-profile-name qp1
OcNOS(config-pon-flow-qos)#exit
```

uni

Use this command to setup UNI parameters of flow like ONU identifier and UNI Port identifier. Onu-id passed in the command should present in the onu list. Check “show pon onu brief” or “show running-config" for configured ONU.

Command Syntax

```
uni
```

Parameters

None

Default

None

Command Mode

PON Flow mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#pon-configuration
OcNOS(config-pon)#flow-id 1
OcNOS(config-pon-flow)#uni
OcNOS(config-pon-flow-uni)#onu-id 0 uni-port-id 0 vlan-tag 20 translation-
profile-name tp1
OcNOS(config-pon-flow-uni)#exit
```

CHAPTER 8 Port Interface Commands

This chapter describes the port interface commands:

fec on

Use this command to change NNI port FEC for 50g/100g speed

FEC will be disabled automatically when speed changed.

Use no form of this command to disable FEC for NNI port.

Command Syntax

```
fec on
no fec
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
(config)#interface nni0/0/1
(config-if)#fec on
(config)#interface nni0/0/1
(config-if)#no fec
```

onu-rogue-detection pon-port

Use this command to enable Rogue ONU detection on a PON port.

Use no form of this command to disable Rogue ONU detection on a PON port.

Command Syntax

```
onu-rogue-detection pon-port IFNAME
no onu-rogue-detection pon-port IFNAME
```

Parameters

IFNAME	PON port interface name

Command Mode

Pon Configuration mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
OcNOS(config-pon)#onu-rogue-detection pon-port pon0/0/1
OcNOS(config-pon)#no onu-rogue-detection pon-port pon0/0/1
```

speed

Use this command to change NNI port speed.

FEC will be disabled automatically when speed changed.

Use no form of this command to restore the default speed for NNI interface.

Command Syntax

```
speed (40g|50g|100g)
no speed
```

Parameters

100g	100 giga bits
40g	40 giga bits
50g	50 giga bits

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
(config)#interface nni0/0/1
(config-if)#speed 100g
(config)#interface nni0/0/1
(config-if)#no speed
```

CHAPTER 9 Show PON commands

This chapter describes the Show PON commands:

- show pon onu uni-port brief
- show pon onu-profile
- show pon onu-profile brief
- show pon qos-profile
- show pon qos-profile brief
- show pon statistics dhcp
- show pon statistics dhcp option-82-pkts
- show pon statistics dhcp rx-pkts
- show pon statistics dhcp tx-pkts
- show pon statistics flow
- show pon statistics flow brief
- show pon statistics flow nni-port
- show pon statistics flow nni-port rx-bytes
- show pon statistics flow nni-port rx-drop-pkts
- show pon statistics flow nni-port rx-pkts
- show pon statistics flow nni-port tx-bytes
- show pon statistics flow nni-port tx-drop-pkts
- show pon statistics flow nni-port tx-pkts
- show pon statistics onu encryption
- show pon statistics onu uni-port
- show pon statistics nni-port
- show pon statistics nni-port brief
- show pon statistics nni-port rx-bytes
- show pon statistics nni-port rx-drop-pkts
- show pon statistics nni-port rx-pkts
- show pon statistics nni-port tx-bytes
- show pon statistics nni-port tx-drop-pkts
- show pon statistics pon-port tx-pkts
- show pon statistics onu uni-port
- show pon statistics pon-port
- show pon statistics pon-port brief
- show pon statistics pon-port rx-bytes
- show pon statistics pon-port rx-drop-bytes
- show pon statistics pon-port rx-pkts
- show pon statistics pon-port tx-drop-bytes
- show pon statistics pon-port tx-pkts
- show pon statistics port brief
- show pon translation-profile
- show pon translation-profile brief

show debugging pon

Use this command to show debugging filters for POND.

Command Syntax

```
show debugging pon
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh debugging pon
  PON State Machine debugging: OFF
  PON Task debugging:          OFF
  PON OMCI debugging:          OFF
  PON NSM client debugging:    OFF
```

show pon acl – all flows

Use this command to show all ACL rules of all flows.

NB: The Applicable rule must have priority, action and direction.

Command Syntax

```
show pon acl all
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon acl all

====================== Flow ID: 1 ======================
 * : to indicate inapplicable rule

 id     priority direction  action      protocol remote-port   remote-ip
 ------------------------------------------------------------------------
 1        10     upstream   drop        tcp      123           1.2.3.4
 2        20     upstream   drop        udp      -             1.2.3.4
 3        30     downstream trap-to-cpu -        -             1.2.3.5
 4        29     downstream allow       -        123           1.2.3.5
 5      * -      -          -           -        -             -
>
```

show pon acl – specific flow

Use this command to show ACL rule(s) of a flow.

NB: The Applicable rule must have priority, action and direction.

Command Syntax

```
show pon acl flowid <0-65536> (aclid <0-65536> |) (downstream|upstream|)
```

Parameters

<0-65535>	Flow Identifier
<0-65535>	ACL Identifier
downstream	Downstream direction
upstream	Upstream direction

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon acl flowid 1
* : to indicate inapplicable rule
id priority direction action protocol remote-port remote-ip
-----------------------------------------------------------------
1 10 upstream drop tcp 123 1.2.3.4
2 20 upstream drop udp - 1.2.3.4
3 30 downstream trap-to-cpu - - 1.2.3.5
4 29 downstream allow - 123 1.2.3.5
5 * - - - - - -
>show pon acl flowid 1 upstream
* : to indicate inapplicable rule
id priority direction action protocol remote-port remote-ip
-----------------------------------------------------------------
1 10 upstream drop tcp 123 1.2.3.4
2 20 upstream drop udp - 1.2.3.4
>
```

show pon acl – trap dump status

Use this command to show ACL trap dump status.

Command Syntax

```
show pon acl dump trap status
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon acl dump trap status
 Dump:         Disabled
 Complete:     No
 Limit:        0MB
 wr-size:      0KB
 wr-packets:   0
 drop-packets: 0
 Flow ID:      0
 ACL Rule ID:  0
 Direction:    upstream
>
```

show pon avail-bw pon-port

Use this command to show PON port available upstream bandwith.

Note: This command is applicable for ASXvOLT16 only.

Command Syntax

```
show pon avail-bw pon-port IFNAME
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
# show pon avail-bw pon-port pon0/0/1
  PON port: pon0/0/1
    CBR_BW(kbps)     TOTAL_BW(kbps)      NEXT_ONU_TOTAL_BW(kbps)
    ------------------------------------------------------------------------------
-----------
    128                       128                               0
```

show pon debug on/off

Use this command to enable/disable POND debugging information filter(s).

Command Syntax

```
show pon debug (pond|state-machine|omci|nsm|all|) on/off
```

Parameters

`all`	POND all information
`nsm`	POND NSM client information
`omci`	POND OMCI information
`pond`	POND task information
`state-machine`	POND State Machine information
`on`	Enable debug information
`off`	Disable debug information

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#show pon debug omci
% POND OMCI debugging is on
```

show pon flow

Use this command to show details for flow.

Command Syntax

```
show pon flow <0-65535> (extra-info)
```

Parameters

`<0-65535>`	FLOW identifier
`extra-info`	Optionally include extra information

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon flow 100
  flow-oper-status:     UP
  pon-port:             pon0/0/1
  uni-end:
    onu-id:             0
    uni-port-id:        0
    trans-profile-name: default_translation_profile
    onu-vlan-tag:       10
  nni-end:
    olt-id:             0
    nni-port-name:      nni0/0/1
    olt-vlan-tag:       20
  qos:
    qos-profile-name:   qp1
  tcont:
    T-CONT-NAME
    -----------
    default_tcont
  gemport:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    default_gemport      0             0        1       1
  acl:
    * : to indicate inapplicable rule

    id     priority direction  action      protocol remote-port   remote-ip
    ------------------------------------------------------------------------

#sh pon flow 100 extra-info
  flow-oper-status:     UP
```

```
pon-port:             pon0/0/1
uni-end:
  onu-id:             0
  uni-port-id:        0
  trans-profile-name: default_translation_profile
  onu-vlan-tag:       10
nni-end:
  olt-id:             0
  nni-port-name:      nni0/0/1
  olt-vlan-tag:       20
qos:
  qos-profile-name:   qp1
tcont:
  T-CONT-NAME
  -----------
  default_tcont
gemport:
  GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
  ------------------------------------------------------------
  default_gemport      0             0        1       1
acl:
  * : to indicate inapplicable rule

  id     priority direction  action      protocol remote-port   remote-ip
  ------------------------------------------------------------------------

ONU Managed Entities:
tcont                                  : 32768
gem_port_net_ctp                       : 1025
ieee_8021_p_mapper_svc_prof            : 10
gem_iw_tp                              : 1025
mac_bridge_port_config_data            : 10
vlan_tag_filter_data                   : 10
ext_vlan_tag_oper_config_data          : 257
pptp_eth_uni                           : 257
priority_queue_g                       : 32769
priority_queue_g                       : 258
ani_g                                  : 32769
gal_eth_prof                           : 1
mac_bridge_svc_prof                    : 257

QoS parameters:
  UPSTREAM-QUEUE  UPSTREAM-SCHEDULER  DOWNSTREAM-QUEUE  DOWNSTREAM-SCHEDULER
  ------------------------------------------------------------------------
  0               0                   0                 20
```

show pon flow brief

Use this command to show all flows.

Command Syntax

```
show pon flow brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show pon flow brief
    FLOW-ID       FLOW-OPER-STATUS
    ------------------------------
    17            UP
    19            UP
```

show pon license

Use this command to show current license information on TIBIT VM.

Command Syntax

```
show pon license
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.1.

Example

```
#show pon license
-----------------------------------------------
PON License Information
-----------------------------------------------
Maximum Licenses     : 8
Available Licenses   : 6
Used Licenses        : 2
```

show pon olt

Use this command to show parameters for configured OLT with particular OLT ID.

Command Syntax

```
show pon olt <0-65535>
```

Parameters

<0-65535>	OLT identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon olt 0
  admin-status:   UP
  oper-status:    UP
  onu-mode:       AUTOMATIC_PROVISION
  dhcp-mode:      OFF
  pon-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED
    ------------------------------------------------------------
    pon0/0/1       UP            UP           -       XG-S
    pon0/0/2       DOWN          DOWN         AD      XG-S
    pon0/1/3       DOWN          DOWN         AD      XG-S
    pon0/1/4       DOWN          DOWN         AD      XG-S
    pon0/2/5       DOWN          DOWN         AD      XG-S
    pon0/2/6       DOWN          DOWN         AD      XG-S
    pon0/3/7       DOWN          DOWN         AD      XG-S
    pon0/3/8       DOWN          DOWN         AD      XG-S
    pon0/4/9       DOWN          DOWN         AD      XG-S
    pon0/4/10      DOWN          DOWN         AD      XG-S
    pon0/5/11      DOWN          DOWN         AD      XG-S
    pon0/5/12      DOWN          DOWN         AD      XG-S
    pon0/6/13      DOWN          DOWN         AD      XG-S
    pon0/6/14      DOWN          DOWN         AD      XG-S
    pon0/7/15      DOWN          DOWN         AD      XG-S
    pon0/7/16      DOWN          DOWN         AD      XG-S
  nni-ports:
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
```

```
                PD - Protocol/Port Down)

    NNI-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  FEC
    ------------------------------------------------------------
    nni0/0/1       UP            UP           -       40G    OFF
    nni0/0/2       UP            DOWN         PD      40G    OFF
    nni0/0/3       UP            DOWN         PD      40G    OFF
    nni0/0/4       UP            DOWN         PD      100G   OFF
```

show pon olt administrative-status

Use this command to show administrative status for configured OLT.

Command Syntax

```
show pon olt <0-65535> adminstrative-status
```

Parameters

`<0-65535>`	OLT identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
>show pon olt 0 adminstrative-status
admin-status: UP
```

show pon olt brief

Use this command to show all configured OLTs.

Command Syntax

```
show pon olt brief
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon olt brief
  OLT-ID           ADMIN-STATUS       OPER-STATUS
  ---------------------------------------------
  0                UP                 UP
```

show pon olt mapping

Use this command to show all discovered OLTs.

Command Syntax

```
show pon olt mapping
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.1.

Examples

```
>show pon olt mapping
Codes: UA - Unassigned
   UNMAPPED OLTs
   OLT-ID          SERIAL
   ----------------------
   UA          e8:b4:70:70:01:3e
```

show pon olt nni-port

Use this command to show specific NNI port for configured OLT.

Command Syntax

```
show pon olt <0-65535> nni-ports WORD
```

Parameters

`<0-65535>`	OLT identifier.
`WORD`	NNI port name.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon olt 0 nni-port nni0/0/1
admin-state:   UP
oper-status:   UP
speed:         40G
fec:           OFF
```

show pon olt nni-port brief

Use this command to show NNI prots for configured OLT.

Command Syntax

```
show pon olt <0-65535> nni-port brief
```

Parameters

<0-65535>	OLT identifier.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon olt 0 nni-port brief
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    NNI-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED  FEC
    ------------------------------------------------------------
    nni0/0/1       UP            UP           -       40G    OFF
    nni0/0/2       UP            DOWN         PD      40G    OFF
    nni0/0/3       UP            DOWN         PD      40G    OFF
    nni0/0/4       UP            DOWN         PD      100G   OFF
```

show pon olt pon-port

Use this command to show specific PON port for configured OLT.

Command Syntax

```
show pon olt <0-65535> pon-port WORD
```

Parameters

`<0-65535>`	OLT identifier.
`WORD`	PON port name.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon olt 0 pon-port pon0/0/1
admin-state:   UP
oper-status:   UP
speed:         XG-S
```

show pon olt pon-port brief

Use this command to show PON ports for configured OLT.

Command Syntax

```
show pon olt <0-65535> pon-port brief
```

Parameters

<0-65535>	OLT identifier.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon olt 0 pon-port brief
    (Reason Code: AD - Admin Down
                  DV - DDM Violation
                  PD - Protocol/Port Down)

    PON-PORT-NAME  ADMIN-STATUS  OPER-STATUS  REASON  SPEED
    ------------------------------------------------------
    pon0/0/1       UP            UP           -       XG-S
    pon0/0/2       DOWN          DOWN         AD      XG-S
    pon0/1/3       DOWN          DOWN         AD      XG-S
    pon0/1/4       DOWN          DOWN         AD      XG-S
    pon0/2/5       DOWN          DOWN         AD      XG-S
    pon0/2/6       DOWN          DOWN         AD      XG-S
    pon0/3/7       DOWN          DOWN         AD      XG-S
    pon0/3/8       DOWN          DOWN         AD      XG-S
    pon0/4/9       DOWN          DOWN         AD      XG-S
    pon0/4/10      DOWN          DOWN         AD      XG-S
    pon0/5/11      DOWN          DOWN         AD      XG-S
    pon0/5/12      DOWN          DOWN         AD      XG-S
    pon0/6/13      DOWN          DOWN         AD      XG-S
    pon0/6/14      DOWN          DOWN         AD      XG-S
    pon0/7/15      DOWN          DOWN         AD      XG-S
    pon0/7/16      DOWN          DOWN         AD      XG-S
```

show pon onu

Use this command to show configuration parameters of ONU.

Command syntax

```
show pon onu <0-4095>
```

Parameters

<0-4095>	ONU identifier.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon onu 0
  pon-port-name:     pon0/0/1
  olt-id:            0
  serial#:           414C5048E3BB8AF9(ALPHE3BB8AF9)
  onu-profile-name:  default_onu_profile
  admin-state:       UP
  oper-status:       UP
  uni-ports:         5
  tcont-maps:
    ALLOC-ID      TCONT-NAME            PON-PORT-NAME
    ------------------------------------------------
    1025          default_tcont         pon0/0/1
  gem-port-maps:
    GEM-PORT-ID   GEM-PORT-NAME         PON-PORT-NAME
    ------------------------------------------------
    1025          default_gemport       pon0/0/1
  onu-flow-list:
    FLOW-ID       FLOW-OPER-STATUS
    ------------------------------
    100           UP
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   CONFIG-IND
    ------------------------------------------------------
    0             UNLOCKED      ENABLED       1G Ethernet full duplex
```

show pon onu admin-status

Use this command to show admin status for configured ONU.

Command Syntax

```
show pon onu <0-4095> admin-status
```

Parameters

`<0-4095>`	ONU identifier.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon onu 0 admin-state
admin-state: UP
```

show pon onu ani-port-power-level

Use this command to show power level on ANI port.

Command Syntax

```
show pon onu <0-4095> ani-port-power-level
```

Parameters

<0-4095>	ONU identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu 0 ani-port-power-level
  ANI-PORT-ID   OPTICAL-SIGNAL-LEVEL(dBm)
  ---------------------------------------
  1             -19.100
```

show pon onu auto finding

Use this command to show all un-provisioned ONUs on different PON ports.

Command Syntax

```
show pon onu unprovisioned
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
#show pon onu unprovisioned
  OLT-ID     PON-PORT     SERIAL#
  -------------------------------
  30         pon30/0/1    49534B5471E81090(ISKT71E81090)
```

show pon onu brief

Use this command to list all configured ONUs.

Command Syntax

```
show pon onu brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu brief
  ONU-ID     OLT-ID   ADMIN-STATE OPER-STATUS     PON-PORT     SERIAL#
  ------------------------------------------------------------------------
  0          0        UP          UP              pon0/0/1
414C5048E3BB8AF9(ALPHE3BB8AF9)
  1          0        UP          UP              pon0/0/1
414C5048E3931006(ALPHE3931006)
```

show pon onu isolated

Use this command to show isolated ONUs on different PON ports. Isolated ONUs remain in isolation list even after reboot.

Command Syntax

```
show pon onu isolated
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Example

```
OcNOS#show pon onu isolated ?
  |  Output modifiers
  >  Output redirection
  <cr>

OcNOS#show pon onu isolated
 Serial Number(Vendor)   PON port
 ---------------------------------
 4142434412345678(ABCD)  pon0/0/1
```

show pon onu mib-audit

Use this command to check MIBs sync between OLT and ONU.

Command Syntax

```
show pon onu <0-4095> mib-audit
```

Parameters

<0-4095>	ONU identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu 0 mib-audit
  MIB-DATA-SYNC-ONU  MIB-DATA-SYNC-OLT  MIB-AUDIT-RESULT
  ------------------------------------------------------
  54                 54                 SYNCED
```

show pon onu olt-id

Use this command to show OLT connected to configured ONU.

Command Syntax

```
show pon onu <0-4095> olt-id
```

Parameters

`<0-4095>`	ONU identifier

Default

By default, there is no domain password.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon onu 0 olt-id
olt-id: 0
```

show pon onu olt-pon-port

Use this command to show OLT's PON port connected to configured ONU.

Command Syntax

```
show pon onu <0-4095> olt-pon-port
```

Parameters

`<0-4095>`	ONU identifier.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon onu 0 olt-pon-port
pon-port-name: pon0/0/1
```

show pon onu onu-profile-name

Use this command to show ONU profile linked to configured ONU.

Command Syntax

```
show pon onu <0-4095> onu-profile-name
```

Parameters

`<0-4095>` ONU identifier

Defaults

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon onu 0 onu-profile-name
onu-profile-name: profile1--1234
```

show pon onu operational-status

Use this command to show operational status for configured ONU.

Command Syntax

```
show pon onu <0-4095> operational-status
```

Parameters

`<0-4095>`	ONU identifier.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

The following example shows setting the administrative distance for all routes.

```
>show pon onu 0 operational-status
oper-status: UP
```

show pon onu queries

Use this command to show ONU queries sent to specific ONU device.

Command Syntax

```
show pon onu <0-4095> queries
```

Parameters

`<0-4095>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

None

show pon onu query brief

Use this command to show all queries sent to all available ONUs.

Command Syntax

```
show pon onu query brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

None

show pon onu rogue

Use this command to show suspected rogue ONUs on different PON ports.

Command Syntax

```
show pon onu rogue
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
# OcNOS#show pon onu rogue ?
  |  Output modifiers
  >  Output redirection
  <cr>

OcNOS#show pon onu rogue
  Serial Number(Vendor)   PON port        Count
  ----------------------------------------------
  -                       pon0/0/1        53
```

show pon onu tcont

Use this command to show details of a T-Cont and the UNI ports & GEM ports connections.

Command Syntax

```
show pon onu <0-4095> tcont WORD
```

Parameters

`<0-4095>` ONU identifier

`WORD` T-CONT name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu 1111 tcont tcont1-1--234
  gem-ports:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    gemport1-1-1-1234    1             3        2       1
    gemport1-1-2--1234   1             3        2       1
```

show pon onu tcont brief

Use this command to show details of all T-Cont and the UNI ports & GEM ports connections.

Command Syntax

```
show pon onu <0-4095> tcont brief
```

Parameters

<0-4095>	ONU identifier

Default

Exec mode

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon onu 1111 tcont brief
  ====================================
  | T-CONT-NAME: tcont1-1--234         |
  ====================================
  gem-ports:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    gemport1-1-1-1234    1             3        2       1
    gemport1-1-2--1234   1             3        2       1
  ====================================
  | T-CONT-NAME: tcont1-2----1234      |
  ====================================
  gem-ports:
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------
    gemport1-2-1-1234    2             3        2       1
    gemport1-2-2-11      2             3        2       1
```

show pon onu tcont gem-port

Use this command to show parameters of a GEM Port.

Command Syntax

```
show pon onu <0-4095> tcont WORD gem-port WORD
```

Parameters

`<0-4095>`	ONU identifier.
`WORD`	T-CONT name
`WORD`	GEM-PORT name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu 1111 tcont tcont1-1--234 gem-port gemport1-1-1-1234
    GEM-PORT-NAME        UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------
    gemport1-1-1-1234    1             3        2       1
```

show pon onu uni-port

Use this command to show details of a specific UNI port.

Command Syntax

```
show pon onu <0-4095> uni-port <0-255>
```

Parameters

<0-4095>	ONU identifier
<0-255>	UNI port identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

```
Example
#sh pon onu 0 uni-port 0
  UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   CONFIG-IND
  ------------------------------------------------
  0             UNLOCKED      ENABLED       1G Ethernet full duplex
```

show pon onu uni-port brief

Use this command to show details of a UNI ports for ONU.

Command Syntax

```
show pon onu <0-4095> uni-port brief
```

Parameters

<0-4095>	ONU identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu 0 uni-port brief
  num-of-unis               : 5
  upstream-priority-queues  : 8
  downstream-priority-queues: 8
  onu-uni-list:
    UNI-PORT-ID   ADMIN-STATUS  OPER-STATUS   CONFIG-IND
    ---------------------------------------------------
    0             UNLOCKED      ENABLED       1G Ethernet full duplex
```

show pon onu-profile

Use this command to show particular configured ONU profile and its parameters.

Command Syntax

```
show pon onu-profile  WORD
```

Parameters

WORD	Translation profile name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon onu-profile onu2_profile-99999999
  ready-status: READY
  onu-tconts:
    T-CONT-NAME
    -----------
    tcont2-1--1234
    tcont2-2
  gem-ports:
    GEM-PORT-NAME        TCONT-NAME           UNI-PORT-ID   P-BITS   US-PQ   DS-PQ
    ------------------------------------------------------------------------------
    gemport2-1-1--12     tcont2-1--1234       1             0        0       0
    gemport2-1-2         tcont2-1--1234       1             1        1       1
    gemport2-2-1-13      tcont2-2             1             2        2       2
    gemport2-2-2         tcont2-2             1             3        3       3
  uni-logic-ports:
    UNI-LOGIC-PORT-ID:
    ------------------
    1
```

show pon onu-profile brief

Use this command to show all configured ONU profiles.

Command Syntax

```
show pon onu-profile brief
```

Parameters

None

Default

By default, the area password is not configured

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon onu-profile brief
  default-onu-profile
  profile1--1234
  profile2-99999999
```

show pon qos-profile

Use this command to show particular configured QoS profile and its parameters.

Command Syntax

```
show pon qos-profile WORD
```

Parameters

WORD	QOS profile name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon qos-profile qosprofile1-12323
  *CIR - Committed Information Rate
  *PIR - Peak Information Rate
  *PBS - Peak Burst Size

  dn-stream-rate-policer:
    CIR      CIR_UNITS      PIR      PIR_UNITS      PBS      PBS_UNITS
    ------------------------------------------------------------------
    11       mbps           2        mbps           2        mbytes
  up-stream-rate-policer:
    CIR      CIR_UNITS      PIR      PIR_UNITS
    ---------------------------------------
    1        mbps           2        mbps
```

show pon qos-profile brief

Use this command to show all configured QoS profiles and their parameters.

Command Syntax

```
show pon qos-profile brief
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon qos-profile brief
default_qos_profile
qosprofile1-12323
qosprofile2---12323
```

show pon statistics dhcp

Use this command to show all DHCP statistics.

Command Syntax

```
show pon statistics dhcp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics dhcp
  DHCPDISCOVER                    :  0
  DHCPOFFER                       :  0
  DHCPREQUEST                     :  0
  DHCPDECLINE                     :  0
  DHCPACK                         :  0
  DHCPNAK                         :  0
  DHCPRELEASE                     :  0
  DHCPINFORM                      :  0
  DHCPV6_SOLICIT                  :  0
  DHCPV6_ADVERTISE                :  0
  DHCPV6_REQUEST                  :  0
  DHCPV6_CONFIRM                  :  0
  DHCPV6_CONFIRM                  :  0
  DHCPV6_RENEW                    :  0
  DHCPV6_REBIND                   :  0
  DHCPV6_REPLY                    :  0
  DHCPV6_RELEASE                  :  0
  DHCPV6_DECLINE                  :  0
  DHCPV6_RECONFIGURE              :  0
  DHCPV6_INFORMATION_REQUEST      :  0
  DHCP_INVALID_REQ                :  0
  DHCP_INVALID_RES                :  0
  DHCP_INVALID_V6                 :  0
  DHCP_PKT_RCV                    :  0
  DHCP_PKT_RCV_ERROR              :  0
  DHCP_PKT_SENT                   :  0
  DHCP_PKT_SEND_ERROR             :  0
  DHCP_OPTION82_INSERTED          :  0
  DHCP_OPTION82_REMOVED           :  0
  DHCP_OPTION82_INSERTION_ERROR   :  0
  DHCP_OPTION82_DELETION_ERROR    :  0
  DHCP_INVALID_PACKET             :  0
  DHCP_FLOW_NOT_FOUND             :  0
  DHCP_IF_NOT_FOUND               :  0
```

show pon statistics dhcp option-82-pkts

Use this command to show DHCP option-82 statistics.

Command Syntax

```
show pon statistics dhcp option-82-pkts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
>show pon statistics dhcp option-82-pkts
  DHCP Option-82 statistics:
    INSERTED        REMOVED         INSERTION-ERROR   DELETION-ERROR
    ------------------------------------------------------------------
    0               0               0                 0
```

show pon statistics dhcp rx-pkts

Use this command to show received DHCP packets number.

Command Syntax

```
show pon statistics dhcp rx-pkts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics dhcp rx-pkts
DHCP rx packets: 0
```

show pon statistics dhcp tx-pkts

Use this command to show transmitted DHCP packets number.

Command Syntax

```
show pon statistics dhcp tx-pkts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics dhcp tx-pkts
DHCP tx packets: 0
```

show pon statistics flow

Use this command to show statistics per specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535>
```

Parameters

<0-65535>	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100
  NNI port: nni0/0/1 Aggregated
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    1113        183743        363         66458         0           0
  UNI port: 0, ONU-ID: 0 Aggregated
    PACKETS         BYTES           DIRECTION
    ----------------------------------------
    363             63554           UPSTREAM
    8               680             DOWNSTREAM
```

show pon statistics flow brief

Use this command to show all flows statistics. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow brief
  ======================
  | FLOW-ID: 100        |
  ======================
  NNI port: nni0/0/1 Aggregated
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    1090        179937        363         66458         0           0
  UNI port: 0, ONU-ID: 0 Aggregated
    PACKETS         BYTES           DIRECTION
    ----------------------------------------
    363             63554           UPSTREAM
    8               680             DOWNSTREAM
```

show pon statistics flow nni-port

Use this command to show statistics for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port
```

Parameters

<0-65535>	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 nni-port
  NNI port: nni0/0/1 Aggregated
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    1138        188049        385         70562         0           0
```

show pon statistics flow nni-port rx-bytes

Use this command to show received bytes for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port rx-bytes
```

Parameters

`<0-65535>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon statistics flow 100 nni-port rx-bytes
  (aggregated) bytes:   195874
```

show pon statistics flow nni-port rx-drop-pkts

Use this command to show rx dropped packets for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port rx-drop-pkts
```

Parameters

`<0-65535>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 nni-port rx-drop-pkts
  (aggregated) dropped packets: 0
```

show pon statistics flow nni-port rx-pkts

Use this command to show received packets for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port rx-pkts
```

Parameters

`<0-65535>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon statistics flow 100 nni-port rx-pkts
  (aggregated) packets: 1157
```

show pon statistics flow nni-port tx-bytes

Use this command to show transmitted bytes for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port tx-bytes
```

Parameters

`<0-65535>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 nni-port tx-bytes
  (aggregated) bytes:   81864
```

show pon statistics flow nni-port tx-drop-pkts

Use this command to show tx dropped packets for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port tx-drop-pkts
```

Parameters

`<0-65535>`	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 nni-port tx-drop-pkts
  (aggregated) dropped packets: 0
```

show pon statistics flow nni-port tx-pkts

Use this command to show transmitted packets for nni-port in specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> nni-port tx-pkts
```

Parameters

<0-65535>	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 nni-port tx-pkts
  (aggregated) packets: 425
```

show pon statistics onu encryption

Use this command to show encryption stats for a specific ONU in a system.

Note: This command is applicable on TIBIT VM.

Command Syntax

```
show pon statistics onu <0-65535> encryption
```

Parameters

<0-65535>	ONU id

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
OcNOS#show pon statistics onu 0 encryption

PON port = pon0/0/1 ONU_ID = 0
        encrypted_bytes  encrypted_pkts          plain_bytes      plain_pkts
-------------------------------------------------------------------------------
TX                16224             338                    0               0
RX                    0               0                16512             344
```

show pon statistics flow uni-port

Use this command to show UNI port Tx,Rx statistics for specific flow. Note that the port statistics for ports associated with flow displays aggregated statistics of port (aggregating stats for all flows associated with the port).

Command Syntax

```
show pon statistics flow <0-65535> uni-port
```

Parameters

<0-65535>	Flow Identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics flow 100 uni-port
  UNI port: 0, ONU-ID: 0 Aggregated
    PACKETS         BYTES           DIRECTION
    ----------------------------------------
    456             80228           UPSTREAM
    8               680             DOWNSTREAM
```

show pon statistics nni-port

Use this command to show stats per specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME
```

Parameters

IFNAME	NNI Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics nni-port nni0/0/1
  NNI port: nni0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    981         161919        271         49394         0           0
```

show pon statistics nni-port brief

Use this command to show stats for all NNI ports in a system.

Command Syntax

```
show pon statistics nni-port brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show pon statistics nni-port brief
  NNI port: nni0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    915         151076        197         35726         0           0
  NNI port: nni0/0/2
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/3
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/4
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
```

show pon statistics nni-port rx-bytes

Use this command to show number of received bytes for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME rx-bytes
```

Parameters

IFNAME	NNI Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
>show pon statistics nni-port nni0/0/1 rx-bytes
Rx bytes:   1001
```

show pon statistics nni-port rx-drop-pkts

Use this command to show number of rx dropped packets for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME rx-drop-pkts
```

Parameters

IFNAME	NNI Port name

Default

By default, max-lsp-lifetime is set to 1200 seconds.

Command Mode

None

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics nni-port nni0/0/1 rx-drop-pkts
Rx dropped packtes:   0
```

show pon statistics nni-port rx-pkts

Use this command to show number of received packets for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME rx-pkts
```

Parameters

IFNAME	NNI Port name

Command Mode

Exec mod

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics nni-port nni0/0/1 rx-pkts
Rx packets: 101
```

show pon statistics nni-port tx-bytes

Use this command to show number of transmitted bytes for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME tx-bytes
```

Parameters

IFNAME	NNI Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics nni-port nni0/0/1 tx-bytes
Tx bytes:   2001
```

show pon statistics nni-port tx-drop-pkts

Use this command to show number of tx dropped packets for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME tx-drop-pkts
```

Parameters

IFNAME	NNI Port name

Default

By default, the maximum number of areas is 3.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics nni-port nni0/0/1 tx-drop-pkts
Tx dropped packtes:   2001
```

show pon statistics nni-port tx-pkts

Use this command to show number of transmitted packets for specific NNI port.

Command Syntax

```
show pon statistics nni-port IFNAME tx-pkts
```

Parameters

IFNAME	NNI Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
>show pon statistics nni-port nni0/0/1 tx-pkts
Tx packets: 201
```

show pon statistics onu uni-port

Use this command to show Tx,Rx statistics on specific UNI port.

Command Syntax

```
show pon statistics onu <0-4095> uni-port <0-255>
```

Parameters

<0-4095>	ONU Identifier
<0-255>	UNI Port identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon statistics onu 0 uni-port 0
  UNI port: 0, ONU-ID: 0
    PACKETS         BYTES           DIRECTION
    ----------------------------------------
    363             63554           UPSTREAM
    8               680             DOWNSTREAM
```

show pon statistics pon-port

Use this command to show stats for specific PON port.

Command Syntax

```
show pon statistics pon-port IFNAME
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#show pon statistics pon-port pon0/0/1
  PON port: pon0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    940         76803         691         33168         0           0
```

show pon statistics pon-port brief

Use this command to show stats for all PON ports in a system.

Command Syntax

```
show pon statistics pon-port brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
show pon statistics pon-port brief
  PON port: pon0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    896         68926         691         33168         0           0
```

show pon statistics pon-port rx-bytes

Use this command to show number of received bytes for specific PON port.

Command Syntax

```
show pon statistics pon-port IFNAME rx-bytes
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics pon-port pon0/0/1 rx-bytes
Rx bytes:   1001
```

show pon statistics pon-port rx-drop-bytes

Use this command to show number of droppped rx packets for specific PON port.

Command Syntax

```
show pon statistics pon-port IFNAME rx-drop-pkts
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics pon-port pon0/0/1 rx-drop-pkts
Rx dropped packets: 0
```

show pon statistics pon-port rx-pkts

Use this command to show number of received packets for specific PON port.

Command Syntax

```
show pon statistics ports pon-port IFNAME rx-pkts
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics pon-port pon0/0/1 rx-pkts
Rx packets: 101
```

show pon statistics pon-port tx-drop-bytes

Use this command to show number of droppped tx packets for specific PON port.

Command Syntax

```
show pon statistics pon-port IFNAME tx-drop-pkts
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#sh pon statistics pon-port pon0/0/1 tx-drop-pkts
Tx dropped packets: 0
```

show pon statistics pon-port tx-pkts

Use this command to show number of transmitted packets for specific PON port.

Command Syntax

```
show pon statistics pon-port IFNAME tx-pkts
```

Parameters

IFNAME	PON Port name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>show pon statistics pon-port pon0/0/1 tx-pkts
Tx packets: 201
```

show pon statistics port brief

Use this command to show stats for all ports in a system.

Command Syntax

```
show pon statistics port brief
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
#sh pon statistics port brief
  PON port: pon0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    875         65260         691         33168         0           0
  NNI port: nni0/0/1
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    873         144098        179         32568         0           0
  NNI port: nni0/0/2
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/3
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
  NNI port: nni0/0/4
    RX-PKTS     RX-BYTES      TX-PKTS     TX-BYTES      RX-DROP-PKT TX-DROP-PKT
    ------------------------------------------------------------------------
    0           0             0           0             0           0
```

show pon translation-profile

Use this command to show specific translation profile.

Command Syntax

```
show pon translation-profile WORD
```

Parameters

WORD	Translation profile name

Default

By default, adjacency-check command is disabled

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#show pon translation-profile default_translation_profile
 ------------------------------------------------------------------------------
                             |         CLASSIFICATION         |     TREATMENT
 TRANS-PROFILE-NAME          | VLAN-TYPE      VLAN-ID  P-BITS | OPERATION    P-BITS
 ------------------------------------------------------------------------------
 default_translation_profile  UNTAGGED       0        0        NONE         0
#
```

show pon translation-profile brief

Use this command to show all configured translation profiles and their parameter values.

Command Syntax

```
show pon translation-profile brief
```

Parameters

None

Default

By default, adjacency-check command is disabled

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#show pon translation-profile brief
  default_translation_profile
```

CHAPTER 10 CMM Show Commands

This chapter describes the CMM-Show commands:

show hardware-information transceiver

Use this command to show XFP transceiver presence, tx, rx states.

Note: This command is applicable for ASXvOLT16 only.

Command Syntax

```
show hardware-information transceiver
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#show hardware-information transceiver

TX     : Transmit status
RX-Los : Receive status
RESET  : Normal (Out of reset), Reset (In reset)
POWER  : Power level Low/High
 -     : NotApplicable

SFP:[0-0]
-----------------------------------------------
PORT   PRESENCE        Tx         Rx-Los
-----------------------------------------------

XFP:[1-16]
-----------------------------------------------
PORT   PRESENCE        Tx         Rx-Los
-----------------------------------------------
1      Present         On         Off
2      Not Present     Off        -
3      Not Present     Off        -
4      Not Present     Off        -
5      Not Present     Off        -
6      Not Present     Off        -
7      Not Present     Off        -
8      Not Present     Off        -
9      Not Present     Off        -
10     Not Present     Off        -
11     Not Present     Off        -
12     Not Present     Off        -
```

```
13      Not Present     Off         -
14      Not Present     Off         -
15      Not Present     Off         -
16      Not Present     Off         -
```

show interface controllers

Use this command to show XFP transceiver EEPROM info.

Note: This command is applicable for ASXvOLT16 only.

Command Syntax

```
show interface (IFNAME|) controllers
```

Parameters

IFNAME	Physical Interface Name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
OcNOS#show interface pon0/0/1 controllers
Codes: SMF - Single Mode Fiber, MMF - Multi Mode Fiber, FC - Fiber Channel
       OM1 - 62.5 Micron MMF [200MHz*km @ 850nm & 500MHz*km @ 1310nm]
       OM2 - 50 Micron MMF [500MHz*km @ 850nm & [500MHz*km @ 1310nm]
       OM3 - 50 Micron MMF [2000MHz*km @ 850nm], OUI - Vendor ID
       OM4 - 50 Micron MMF [4700MHz*km @ 850nm], BR - Bit Rate, CC - Check Code
       AOC - Active Optical Cable, ACC -  Active Copper Cable, PC - Power Class
       CDR - Clock Data Recovery, CLEI - Common Language Equipment Identification
       LR - Long Reach, SR - Short Reach, IR - Intermediate Reach
       CCA - Copper Cable Attenuation

Port Number                   : 1
Name                          : Hisense
OUI                           : 0x0 0x0 0x0
Part No                       : LTH7226-PC+
Serial_Number                 : H278CZ00014
Identifier                    : XFP
Ext. Identifier               : Power Level 3 (3.5W Max)
                                Non-CDR version
                                TX Ref Clock Input Not Required
Connector Type                : SC (Subscriber Connector)
10G Ethernet Compliance       :
10G Fiber Channel Compliance  :
10G Copper Links              :
Lower Speed links             :
SONET Codes - Interconnect    :
SONET Codes - Short Haul      :
SONET Codes - Long Haul       :
SONET Codes - Very Long Haul  :
```

```
Length SMF                     : 20 (Kilometers)
Length OM1                     : 0 (Meters)
Length OM2                     : 0 (Meters)
Length OM3                     : 0 (X 2 Meters)
Length OM4 / Cable Assembly    : 0 (X 1 Meters (For Copper or AOC) / X 2 Meters (for OM4))
Revision Level                 : 01
Manufacturing Date             : 181225   (yymmddvv, v=vendor specific)
Encoding Algorithm             : 64B/66B,NRZ
CC                             : 0x10
CC Ext.                        : 0xf5
Nominal BR                     : 99 (X 100 Mbps)
Max BR                         : 99
Min BR                         : 99
Max Case Temperature           : 75.00C
Options Implemented            : Soft TX_DISABLE implemented
Device Technology              : No Wavelength Control
                                 APD Detector
                                 Transmitter Not Tunable
                                 Cooled Transmitter
                                 Copper Cable, Linear Active Equalizers
CDR support                    : CDR support for 9.95 Gb/s
Voltage monitored by AUX       :
wavelength                     : 1577nm
Wavelength Tolerance           : 5nm
DDM Support                    : Yes
```

show interface transceiver

Use this command to show XFP rx/tx power level, temperature, current and voltage values and alarm thresholds.

Note: This command is applicable for ASXvOLT16 only.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violations|)
```

Parameters

IFNAME	Physical Interface Name
detail	Transceiver info such as volt,temp,power and current
threshold violations	Threshold violation info

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Example

```
OcNOS#show interface pon0/0/1 transceiver detail
Codes:     * Not Supported by device        -- No Power

Intf       DDM        Lane       Temp       AlertMax   CritMax    CritMin    AlertMin
                                 (Celsius)  (Celsius)  (Celsius)  (Celsius)  (Celsius)
-------------------------------------------------------------------------------------
pon0/0/1   Inactive   -          +30.28     +85.00     +78.00     -8.00      -15.00

Intf       DDM        Lane       Volt       AlertMax   CritMax    CritMin    AlertMin
                                 (Volts)    (Volts)    (Volts)    (Volts)    (Volts)
-------------------------------------------------------------------------------------
pon0/0/1   Inactive   -          +3.336     +3.630     +3.470     +3.130     +2.970

Intf       DDM        Lane       Curr       AlertMax   CritMax    CritMin    AlertMin
                                 (mA)       (mA)       (mA)       (mA)       (mA)
-------------------------------------------------------------------------------------
pon0/0/1   Inactive   -          +41.454    +70.000    +65.000    +0.500     +0.000

Intf       DDM        Lane       RxPwr      AlertMax   CritMax    CritMin    AlertMin
                                 (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------------------
pon0/0/1   Inactive   -           --       -4.000     -5.000     -29.586    -30.458

Intf       DDM        Lane       TxPwr      AlertMax   CritMax    CritMin    AlertMin
                                 (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------------------
pon0/0/1   Inactive   -         +1.054     +4.990     +3.990     -2.010     -3.010
```

SECTION 19 Glossary

Glossary

Conventions

This document uses the conventions described below.

Sort Order

The terms are arranged in ASCII order with the case of the characters ignored. This is the same as if the terms were sorted by this Linux command:

sort -f

This means that spaces, symbols, and digits come before alphabetic characters. Digits are sorted as strings, not numeric values (“10” comes before “2”).

The exact ASCII collating sequence is as shown below, with a space character in the first position:

```
 !"#$%&'()*+,-./
0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

There are some exceptions to this rule when it makes more sense than strict ASCII order:

- (S,G) is under S
- G.8032 and G.8032 are under Numbers

Acronyms

The full phrase is shown before the acronym. For example:

- network address translation (NAT)
- Local Area Network (LAN)

An exception is when the acronym is used exclusively to refer to the term, in which case the acronym is shown before the full form:

- I-SID (Service Instance Identifier)
- NETCONF (Network Configuration Protocol)

When an acronym is part of a phrase and is defined separately, its full form is not shown:

- BGP confederation
- FEC-to-NHLFE (FTN) map
- GARP VLAN Registration Protocol (GVRP)
- MAC address

Case

As shown in the examples above, all lowercase is used for terms except when the predominant usage is initial uppercase or all uppercase.

Terms

Numbers

1588v2. IEEE specification for Precision Time Protocol (PTP).

802. A family of IEEE Local Area Network (LAN) standards. The services and protocols specified by the 802 standards map to Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model:

- 802.1: Overview architecture of LANs and interneworking
- 802.2: The logical link control (LLC) sublayer of Layer 2 (L2)
- 802.3: Layer 1 (L1) and the Media Access Control (MAC) sublayer of Layer 2 (L2), Also called Ethernet.

802.1AB. IEEE specification for Link Layer Discovery Protocol (LLDP).

802.1ad. Amendment to IEEE 802.1Q for Provider Bridging (PB).

802.1ag. Amendment to IEEE 802.1Q for Connectivity Fault Management (CFM).

802.1ah. IEEE specification that adds Provider Backbone Bridging (PBB) to 802.1ad Provider Bridging (PB):

802.1ak. Amendment to IEEE 802.1Q for Multiple Registration Protocol (MRP).

802.1aq. Amendment to IEEE 802.1D for Shortest Path Bridging (SPB).

802.1AX. IEEE specification for link aggregation and Multi-Chassis Link Aggregation (MC-LAG).

802.1D. IEEE specification which allows multiple LANs to be connected together through what the standard calls a “MAC bridge” which filters data sent between LAN segments, allowing networks to be partitioned for administrative purposes and reducing network congestion. The more common term for a MAC bridge is switch. The 802.1D standard includes Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

802.1p. IEEE 802.1Q defines priority signaling for traffic that can be used by Quality of Service (QoS) mechanisms to differentiate traffic. Packets are tagged as belonging to a queue, which determines the priority of the packet. Although this technique is often called “802.1p”, there is no standard by that name. Instead, the technique is incorporated into 802.1Q standard.

802.1Q. IEEE Virtual Local Area Network (VLAN) and Multiple Spanning Tree Protocol (MSTP) specifications. This standard refers to VLANs as “virtual bridged networks”. The 802.1D standard covers “VLAN-unaware” switches, while 802.1Q extends 802.1D for “VLAN-aware” switches.

802.1Qau. Amendment to IEEE 802.1Q for Quantized Congestion Notification (QCN).

802.1Qay. Amendment to IEEE 802.1Q for Provider Backbone Bridge-Traffic Engineering (PBB-TE).

802.1Qaz. Amendment to IEEE 802.1Q for Data Center Bridging Capability Exchange (DCBX) and Enhanced Transmission Selection (ETS).

802.1Qbb. Amendment to IEEE 802.1Q for Priority-based Flow Control (PFC).

802.1Qbg. Amendment to IEEE 802.1Q for Edge Virtual Bridging (EVB).

802.1v. Amendment to IEEE 802.1Q to classify incoming packets based on data link layer protocol identification.

802.3ah. IEEE specification for Ethernet to the First Mile (EFM).

802.3x. IEEE specification for flow control.

G.8032. ITU-T specification for Ethernet Linear Protection Switching (ELPS).

G.8032. ITU-T specification for Ethernet Ring Protection Switching (ERPS).

A

Access Control List (ACL). A set of rules used to filter traffic. Each rule specifies a set of conditions (such as source address, destination address, type of packet, or combination of these items) that a packet must meet to match the rule. When a device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied.

access layer. In the network design model, the layer that connects devices such as desktops, laptops, servers, and printers to the network and provides end users access to network resources. This layer accepts traffic into a network and can pass that traffic to the distribution layer. The access layer is usually built using Layer 2 (L2) switching such as Spanning Tree Protocol (STP). This layer connects logical broadcast domains and provides isolation to groups of users. Typically, Virtual Local Area Network (VLAN) instances are implemented as broadcast domains in the access layer. Also called the edge layer. See also customer edge (CE), provider edge (PE).

acknowledgment (ACK). Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred.

active route. Route chosen from all routes in a Routing Information Base (RIB) to reach a destination. Active routes are installed in the Forwarding Information Base (FIB).

address. A unique identifier for a device on a network, either as a sender or receiver. An address can be a physical address or a logical address.

See also address family, address resolution, Classless Interdomain Routing (CIDR), domain name, Domain Name Service (DNS), dynamic address, IP address, MAC address, name resolution, static address.

address family. A specific type of network addressing supported by a routing protocol. Examples are IPv4 unicast and IPv4 multicast.

address resolution. The process of translating the address of an entity on one system to the equivalent address of the same entity on another system. For instance, translating an IP address to its Domain Name Service (DNS) name. See also Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP). A Transmission Control Protocol/Internet Protocol (TCP/IP) mechanism that maps a MAC address to an IP address in the ARP cache data structure. Defined in RFC 826. See also Neighbor Discovery Protocol (NDP).

adjacency. The relationship between neighboring devices for exchanging routing information. Adjacent devices share a common network segment.

A given device can have multiple adjacencies, but each adjacency consists of only two devices connected by one link. A protocol data unit (PDU) that goes between them does not have to pass through any other network devices. See also neighbor.

administrative distance. How reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the Routing Information Base (RIB). Also called route preference.

Advanced Encryption Standard (AES). A cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. Defined in Federal Information Processing Standards (FIPS) PUB 197.

advertising. Process in which routing or service updates are sent at specified intervals so that other devices on the network can maintain lists of usable routes.

Agent Extensibility (AgentX). A protocol used to implement Simple Network Management Protocol (SNMP) that defines communications between an SNMP agent and an SNMP client. AgentX does not directly communicate with an SNMP client, but relies on the agent to handle the protocol details of SNMP. Defined by RFC 2741.

aggregate route. A single entry in a routing table that represents a combination of groups of routes that have common addresses. See also route summarization.

alarm indication signal (AIS). A signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving device that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute (ANSI). A voluntary organization of corporate, government, and other members that develops international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

application-specific integrated circuit (ASIC). An integrated circuit that is designed for a specific application.

area. A logical division of devices that maintains detailed routing information about itself as well as routing information that allows it to reach other routing subdomains. An area divides a network into small, manageable pieces, reducing the amount of information each device must store and maintain about all other devices.

In Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF), an area is a set of contiguous networks and hosts within an autonomous system (AS) that have been administratively grouped together.

area border router (ABR). A router on the border of one or more Open Shortest Path First (OSPF) areas that connects those areas to the backbone network. An ABR is a member of both the OSPF backbone and its attached areas. Therefore, an ABR maintains routing tables for both the backbone topology and the topology of the other areas. See also Not-So-Stubby-Area (NSSA), stub area.

authentication. A process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

authentication, authorization, and accounting (AAA). A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the network
- Authorization determines what the user can do
- Accounting tracks the user's activities and provides an audit trail that can be used for billing or resource tracking

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

Authentication Header (AH). An Internet Protocol Security (IPsec) protocol that authenticates either all or part of the contents of a packet by adding a header with a a hash message authentication code (HMAC) calculated based on the values in the packet. AH provides authentication but not confidentiality. See also Encapsulating Security Payload (ESP).

Automatic Protection Switching (APS). A means to detect a signal failure or signal degrade on a working channel and switch traffic to a protection channel. There are two types of APS:

- Ethernet Linear Protection Switching (ELPS)
- Ethernet Ring Protection Switching (ERPS)

autonomous system (AS). A network controlled as a single administrative entity sharing a common routing strategy. An autonomous system is subdivided into areas. An AS runs an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Intermediate System to Intermediate System (IS-IS) within its boundaries. An AS uses an Exterior Gateway Protocol (EGP) to exchange routing information with other ASs.

autonomous system border router (ASBR). An area border router (ABR) located between an Open Shortest Path First (OSPF) autonomous system (AS) and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as Routing Information Protocol (RIP).

An ASBR is a link between the OSPF autonomous system and the outside network. An ASBR exchanges routing information with routers in other ASes. The ASBR redistributes routing information received from other ASs throughout its own AS. An ASBR must reside in a standard OSPF area.

availability. The amount of time that a system is available during time periods when it is expected to be available. Availability is often measured as a percentage of an elapsed year. For example, 99.95% availability equates to 4.38 hours of downtime in a year (0.0005 * 365 * 24=4.38) for a system that is expected to be available all the time.

B

B-MAC. A source and destination backbone MAC address (B-AA and a B-DA) in a Provider Backbone Bridging (PBB) header.

B-TAG. See backbone VLAN (B-VLAN).

backbone. The part of a network used as the primary path for transporting traffic between network segments.

backbone core bridge (BCB). A device that bridges frames based on backbone VLAN (B-VLAN) and backbone MAC address (B-MAC) information in a Provider Backbone Bridging (PBB) network core.

backbone edge bridge (BEB). A device that encapsulates customer frames for transmission across a Provider Backbone Bridging (PBB) network. There are two types:

- B-BEB (B type BEB): Contains a B-component for bridging in the provider space based on backbone MAC address (B-MAC) and backbone VLAN (B-VLAN) information.
- I-BEB (I type BEB): Contains an I-component for bridging in the customer space based on customer MAC address (C-MAC) and service VLAN (S-VLAN) information.

backbone VLAN (B-VLAN). A field in a Provider Backbone Bridging (PBB) header that carries the backbone VLAN identifier information. The format is the same as a service VLAN (S-VLAN) tag. Also called B-VID tag, B-TAG.

backhaul. The part of a hierarchical network that connects small subnetworks at the edge of the network to the core or backbone network.

In wireless backhaul, the part of the network that transports traffic from a cellular base station to a core network that routes and switches voice and data traffic.

bandwidth. A measure of the data transfer rate of a communications transport medium.

base station. An earth-based transmitting/receiving station for cellular phones and other wireless transmission systems.

Bellman-Ford algorithm. Used in distance-vector routing protocols such as Routing Information Protocol (RIP) to determine the best path to all routes in the network. Contrast with Dijkstra algorithm.

best effort. Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets not explicitly assigned to a specific traffic class are assigned to the best-effort class.

BGP confederation. A method to solve scaling problems created by the iBGP full-mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number.

Within a sub-AS, the same iBGP full mesh requirement exists. Connections to other confederations are made with eBGP, and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.

BGP neighbor. Another device on the network that is running Border Gateway Protocol (BGP). There are two types of BGP neighbors: internal neighbors in the same autonomous system (AS) and external neighbors in different autonomous systems.

BGP peer. A remote Border Gateway Protocol (BGP) speaker that is an established neighbor of the local BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP speaker. A router configured to run the Border Gateway Protocol (BGP) routing protocol. A BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection (BFD). Protocol that reduces the reliance upon the relatively slow hello mechanism in routing protocols to detect failures where no hardware signaling is available. BFD works with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) v2, and Intermediate System to Intermediate System (IS-IS) to enable them to receive failure notifications. Defined in RFCs 5880 and 5881.

bit error rate (BER). The ratio of error bits to the total number of bits transmitted. A BER is generally shown as a negative exponent (for example, 10-7, which means one out of 10,000,000 bits is in error).

Border Gateway Protocol (BGP). An Exterior Gateway Protocol (EGP) that maintains a table of IP networks, or prefixes, which designate network reachability among autonomous system (AS) instances. BGP uses path-vector routing that makes decisions based on path, network policies, and/or rule sets. BGP is the primary protocol for the global Internet. First defined by RFC 1163.

BGP Version 4 (BGP4) defined in RFC 4271 supports Classless Interdomain Routing (CIDR) and route summarization.

BGP performs these tasks:

- Collects information about reachable networks from neighboring autonomous systems

- Advertises its reachable networks to routers inside the AS and to neighboring autonomous systems
- Selects routes if there are multiple routes available.

Each BGP device can have both external and internal connections to other BGP devices:

- Internal BGP (iBGP) connections are within the same autonomous system
- External BGP (eBGP) connections are between different autonomous systems

The configuration and behavior is slightly different between eBGP and iBGP.

You can use iBGP for multihomed BGP networks (with more than one connection to the same external autonomous system).

To avoid routing loops, iBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full-mesh requirement becomes difficult to manage. To combat scaling problems, BGP uses route reflection and BGP confederations.

Multiprotocol BGP (MP-BGP) allows different types of addresses (address families) to be distributed in parallel. MP-BGP supports IPv4 and IPv6 addresses as well as unicast and multicast variants of each. Defined in RFC 4760. See also IPv6 Provider Edge (6PE).

See also community.

bridge. A device operating at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model that forwards frames from one network segment to another based on the MAC address.

The term bridge also describes a device that connects collision domains. Collisions that appear on one side of a switch are not allowed to propagate to the other.

Originally, bridges only had two ports, with each one connected to a network segment. Later, bridges had multiple ports that could connect more than two network segments as well as directly connecting hosts. As bridges evolved, they were also able to filter frames, that is, forward only certain traffic from one network segment to another. This type of device is sometimes called an intelligent bridge, but the more modern term is switch. The term “bridge” is somewhat archaic but is still often used in standards documents.

bridge protocol data unit (BPDU). A protocol data unit (PDU) sent by switches running the Spanning Tree Protocol (STP) to learn about other switches in the network and maintain the spanning tree.

broadcast. The process of a single host simultaneously sending the same message to all nodes on a network. Compare to multicast, where a only a subset of the receivers are addressed. See also unicast.

bursty. The tendency of the bandwidth needed in a network to vary greatly from one moment to the next.

C

C-MAC. A source and destination customer MAC address (C-SA and a C-DA) in a Provider Backbone Bridging (PBB) header.

C-TAG. See customer VLAN (C-VLAN).

Carrier Ethernet. Extensions to Ethernet that enable network operators to provide Ethernet services to customers and to use Ethernet technology in their networks. See also Metro Ethernet Forum (MEF).

certificate. Electronic document that identifies a person or entity. Through the use of keys and certificates, the entities exchanging data can authenticate each other.

channel. A connecting path that carries information from a sending device to a receiving device. A channel can refer to a physical medium (such as a coaxial cable or fiber optic cable).

circuit. A communications channel or path between two devices capable of carrying electrical current.

circuit switching. A network where a dedicated circuit must be opened between devices before they can communicate and, while the circuit is open, no other devices may use that circuit or parts of it. A circuit can remain open without any information transmission, and still be unusable by other devices; it must be closed before it is available to other users. Contrast with packet switching.

Class of Service (CoS). A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, video, voice, file transfer) together and treating each type as a class with its own level of service priority. However, no guarantees are made that a given priority will meet any specified minimum level. See also Quality of Service (QoS).

classful IP addressing. An older addressing scheme for configuring the ratio of networks to hosts using fixed length prefixes. See Classless Interdomain Routing (CIDR).

Classless Interdomain Routing (CIDR). A notation for specifying an IP addresses and its network prefix which appends a slash character to the address and a decimal number indicating the leading bits in the network prefix. For example:

- In the IPv4 notation “192.168.0.0/16”:
  - “192.168” (the first 16 bits) defines the network address.
  - .0.0 up to .255.255 refer to the host addresses on that network. This leaves 16 bits to contain host addresses, enough for 65536 host addresses.
- In the IPv6 notation “2001:db8::/32”:
  - “2001:db8” (the first 32 bits) defines the network address.
  - :0:0:0:0:0:0 to:ffff:ffff:ffff:ffff:ffff:ffff refer to host addresses on that network. This leaves 96 bits to contains host addresses, enough for 7,922,816,251,426,433 host addresses.

The lower the number after the slash, the more hosts contained in that block.

CIDR uses variable length subnet masking (VLSM) based on arbitrary length prefixes. In VLSM, the number of network and host bits assigned to a subnet can vary based on the number of hosts the subnet needs to support.

CIDR replaced traditional classful IP addressing, in which address allocation was based on octet (8-bit) boundary segments of the IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary. The old classful A, B, and C network designations correspond to CIDR prefixes of /8, /16, or /24. 192.168.0.0/16 corresponds to an old class B network. With CIDR, finer grained division of networks are possible, down to individual IP addresses, such as 192.168.100.2/32.

CIDR routes can be carried by Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Before CIDR notation, IPv4 networks were represented using dotted decimal notation for both the address and a subnet mask.

Also called route summarization or supernetting.

client/server architecture. A computing architecture that distributes processing between clients and servers on the network. A client program makes a service request from a server which fulfils the request.

collapsed core. Collapsing the core layer and the distribution layer into one layer (one device) in the network design model. A collapsed core design reduces cost, while maintaining most of the benefits of the network design model for small networks that do not grow significantly larger over time.

collision domain. A network segment where data frames can collide with one another when being sent on a shared medium such as Ethernet. Hosts in a collision domain arbitrate among themselves using an access control mechanism.

command-line interface (CLI). Environment for entering commands to configure and monitor routing and switching software and hardware.

committed information rate (CIR). The average rate at which packets are admitted to the network. Each packet is counted as it enters the network. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority.

common and internal spanning tree (CIST). A single topology connecting all Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) switches into one active topology. In other words, an entire spanning tree fabric.

common spanning tree (CST). The topology connecting all Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) *switches* and multiple spanning-tree (MST) region *instances*. An MST region appears as a single switch to spanning tree configurations outside the region.

community. In Border Gateway Protocol (BGP), a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems.

In Simple Network Management Protocol (SNMP), an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which Management Information Base (MIB) objects are available, and specifies the operations (read-only or read-write) allowed on those objects.

congestion. The state in which the network load exceeds the available resources such as link capacity or memory buffers.

connection-oriented. A packet switching technology where a virtual circuit between sending and receiving devices makes it seem like the devices are connected by a switched circuit with a fixed bandwidth without regard to their physical addresses. In a connection-oriented service, packets always reach their destination in the same order as they were sent. Transmission Control Protocol (TCP) is a connection-oriented transport service. See also connectionless.

Connection-oriented protocols can be used to send information that requires a constant delay and bandwidth such as voice and video.

connectionless. A packet switching technology where the source and destination addresses are included in each packet so that a direct connection or an established session between sender and receiver is not required for communications. In a connectionless service, each packet is handled independently of all others, and packets might not reach their destination in the same order in which they were sent. User Datagram Protocol (UDP) is a connectionless transport service. See also connection-oriented.

Connectivity Fault Management (CFM). An Operation, Administration, and Maintenance (OAM) protocol that can manage Ethernet services and detect, verify, and isolate connectivity failures in VLANs. CFM enables service providers to configure:

- Maintenance association End Point (MEP) on a per-port, per-VLAN, or per-domain basis
- Maintenance domain Intermediate Point (MIP) on a per-port and per-level basis

CFM can operate over a LAN segment, customer VLAN (C-VLAN), service VLAN (S-VLAN), backbone VLAN (B-VLAN), or backbone identified by an I-SID (Service Instance Identifier). Defined by IEEE 802.1ag and 802.1ah.

Constrained Shortest Path First (CSPF). An extension of shortest path first (SPF). The path computed using CSPF is the shortest path that fulfills a set of constraints. After running the shortest path algorithm, the paths are pruned, removing those links that violate a given set of constraints.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Content Addressable Memory (CAM). An integrated circuit in a device that stores a table used to make frame forwarding and classification decisions. CAM can perform a massively parallel search of entries in the table much faster than a serial search than in conventional Random Access Memory (RAM).

There are two types of CAM:

- Binary CAM: A binary lookup that returns either a 1 or 0. A MAC address in an Ethernet frame comes into a switch, the switch looks in its MAC address table and either finds that MAC address or does not (1 or 0).
- Ternary CAM (TCAM): A binary lookup that returns either a 1 or 0 but also has a “do not care” bit. TCAM can have multiple matches and can determine a best match. This is necessary because Classless Interdomain Routing (CIDR) lookups need a longest prefix match. For example, 192.168.1.7/32 matches both 192.168.1.0/24 and 192.168.1.0/25. The closest match to 192.168.1.7/32 is 192.168.1.0/25 which would be chosen.

Continuity Check Message (CCM). A multicast Connectivity Fault Management (CFM) protocol data unit (PDU) transmitted periodically by a Maintenance association End Point (MEP) in ensure continuity over the Maintenance Association (MA) to which the transmitting MEP belongs.

control plane. The part of switch or router architecture that makes decisions about where traffic is sent. Control plane processing is the “signalling” of the network. Anything that is needed to get routing and switching working on a device is considered part of the control plane. The control plane serves the data plane.

The control plane functions include the manual system configuration and management operations performed by a network administrator. The control plane functions also include dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP) that exchange topology information with other routers and construct a Routing Information Base (RIB).

The control plane functions are not performed on each arriving individual packet, so they do not have a strict speed constraint and are not time-critical.

Control plane packets are sent to or are locally originated by the device itself.

convergence. The synchronization process that a network must go through immediately after a topology change. Convergence time is the time required to update all the devices on the network with the routing information changes. See also routing table.

core layer. In the network design model, the layer that provides a transit function to access the internal network and external networks. The core layer moves packets between distribution layer devices. The core layer also links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

The core layer uses Layer 3 (L3) routing protocols that scale well and converge quickly such as Open Shortest Path First (OSPF).

The core serves as the backbone for the network and is critical for connecting distribution layer devices, so it is important for the core to be fast with low-latency, reliable, and scalable.

Also called backbone or trunk.

count-to-infinity. A distance-vector routing problem where if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

The count-to-infinity problem is caused by a link failure that partitions the network into two or more segments. When the network is partitioned, devices in one part of the segment cannot reach devices in the other part of the segment. The distance-vector algorithm adjusts the distance value slowly upwards toward infinity.

The count-to-infinity problem can be solved through split horizon methods.

cryptography. Rendering information unintelligible and restoring encrypted information to an intelligible form.

customer edge (CE). A device that provides an interface between a Local Area Network (LAN) and an enterprise or service provider core network. Outbound packets from the LAN are forwarded from the CE to a provider edge (PE) device, and inbound packets are forwarded from the PE to the CE.

customer VLAN (C-VLAN). In a Provider Bridging (PB) frame, a field that identifies the customer VLAN. See also service VLAN (S-VLAN). Also called C-TAG.

D

daemon. A background program that runs unattended and is usually invisible to users and that provides important system services. Pronounced “dee-mon” or “day-mon”.

Data Center Bridging (DCB). A collection of extensions for Ethernet that allows LANs and Storage Area Networks (SANs) to use a single unified fabric in a data center. DCB can carry Fibre Channel, TCP/IP, and inter-process communication traffic over a single, converged Ethernet network. DCB features include:

- Priority-based Flow Control (PFC)
- Enhanced Transmission Selection (ETS)
- Quantized Congestion Notification (QCN)
- Data Center Bridging Capability Exchange (DCBX)

Data Center Bridging Capability Exchange (DCBX). Defined in IEEE 802.1Qaz, a protocol that uses Link Layer Discovery Protocol (LLDP) to convey configuration of Data Center Bridging (DCB) features between neighbors.

data communications equipment (DCE). The interface between data terminal equipment (DTE) and a network.

Data Encryption Standard (DES). A method of data encryption using a private (secret) key. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among these. Both the sender and the receiver must know and use the same private key.

In triple DES (3DES), a symmetric-key block cipher applies the DES cipher algorithm three times to each data block.

data link layer. See Layer 2 (L2).

data plane. The part of switch or router architecture that forwards frames and packets arriving on an interface. Routers and switches use what the control plane has built to process incoming frames and packets. The data plane forwards traffic to the next hop along the path to the destination according to the control plane logic. Data plane frames or packets go *through* the device.

Also called forwarding plane.

data terminal equipment (DTE). Any device such as a host, router, or switch connected to a network. A DTE connects to a network through data communications equipment (DCE).

default gateway. A router that connects hosts on a network segment to the Internet.

default route. A route used to forward Internet Protocol (IP) packets when a more specific route is not present in the Routing Information Base (RIB). Often represented as 0.0.0.0/0, the default route is sometimes called the “route of last resort”.

Differentiated Services (DiffServ). A mechanism to classify and manage network traffic and provide Quality of Service (QoS) guarantees for service providers. DiffServ extends the Resource Reservation Protocol—Traffic Engineering (RSVP-TE). DiffServ enables traffic to be prioritized by class, so that certain kinds of traffic, for example voice traffic, can take precedence over other types of traffic.

DiffServ redefines bits in the type of service (ToS) field of an IP packet header. DiffServ uses the Differentiated Services Code Point (DSCP) field for the QoS priority and supports 64 levels of classification.

Defined by RFC 2474; Multi-Protocol Label Switching (MPLS) support is defined in RFCs 3270 and 4124.

Differentiated Services Code Point (DSCP). A six-bit field in an IP header that enables service providers to allocate resources on a per-packet basis to meet customer requirements. See also Differentiated Services (DiffServ).

Diffie–Hellman. A method of securely exchanging cryptographic keys that allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature Algorithm (DSA). An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Dijkstra algorithm. An algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on link state. Also called shortest path first (SPF). Contrast with Bellman-Ford algorithm.

distance-vector routing. A family of routing algorithms that calculate the best route to use to send data based on information from adjacent (directly connected) routers on the network.

“Distance-vector” means that routes are advertised with two characteristics:

- Distance: How far it is to the destination based on a metric such as the number of hops, cost, bandwidth, or delay.
- Vector: The direction (exit interface) of the next hop router to reach the destination.

Each router sends its neighbors a list of networks it can reach and the distance to that network. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its Routing Information Base (RIB). These best paths are advertised to each adjacent router.

Routing information is broadcast periodically rather than only when a change occurs, which makes the method compute- and bandwidth-intensive. For this reason, a distance-vector algorithm is best used in relatively small networks with few interrouter connections.

The Bellman-Ford algorithm is often used to determine the best path, which is used by the Routing Information Protocol (RIP).

Distance-vector routing can be prone to routing loops which are avoided through split horizon techniques.

Contrast with link-state routing and shortest-path routing.

distribution layer. In the network design model, the layer that aggregates the data received from the access layer and sends it to the core layer or to other segments of the local network. Routers or multilayer switches in the distribution layer performs many functions including:

- Routing between subnetworks and Virtual Local Area Network (VLAN) instances in the access layer
- Managing access control, routing, filtering, and QoS policies
- Managing firewalls and network address translation (NAT)
- Managing queues and prioritizing traffic
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions

The distribution layer uses Layer 3 (L3) routing to connect to the core layer and Layer 2 (L2) switching to connect to the access layer.

Also called the aggregation layer or concentration layer.

domain. A representation of all or a subset of a network used for addressing and administrative purposes. Also refers to a collection of routers that use a common Interior Gateway Protocol (IGP). See also area and autonomous system (AS).

domain name. A meaningful and easy-to-remember name for an IP address. A domain name is a sequence of names (labels) separated by periods such as “example.com”.

Domain Name Service (DNS). A service that translates a domain name into a numeric IP address needed to locate devices. The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation exchanges within the DNS hierarchy, the IP address for the given host eventually arrives at the client. Defined in RFCs 1034 and 1035.

dotted decimal. A method of representing an IPv4 address as four decimal numbers separated by dots, or periods; for example, 194.65.87.3. See also IP address.

double colon. A notation used to represent a consecutive block of zeroes in the middle of an IPv6 address. For example, given this address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

With double colon notation, the address shown above becomes:

FE80::0202:B3FF:FE1E:8329

You can only use the double colon notation once in an address.

double tagged. See Provider Bridging (PB).

dynamic address. An address assigned to a device on a network with no regard to matching a specific address to that device. When a client device (such as a laptop) is given a dynamic address, it simply receives one from a pool of available addresses. It might or might not be allocated the same IP address as on previous connections. See also Dynamic Host Configuration Protocol (DHCP).

Dynamic Host Configuration Protocol (DHCP). A protocol where a client can obtain an IP address and other information such as default gateway, subnet mask, and Domain Name Service (DNS) servers, for the client to use to connect to a network. Defined in RFCs 2131 and 3315. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

A DHCP server “leases” an IP address for a predetermined period of time, and reclaims the address for reassignment at the expiration of that period. DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops, tablets, and smart phones frequently join and leave.

dynamic routing. A technique used by routing protocols where devices send and receive messages about the network topology to and from other devices and update a local Routing Information Base (RIB) used to locate the best available path to a destination.

There are different forms of dynamic routing: distance-vector routing, link-state routing, and path-vector routing. Several protocols use dynamic routing such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Also called adaptive routing. Contrast with static routing.

E

east/west. The flow of traffic traversing a data center or cloud horizontally between servers. Contrast with north/south.

Edge Virtual Bridging (EVB). A mechanism that enables a virtual switch to send all traffic to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB leverages the advanced management capabilities in access or aggregation layer switches. Defined by IEEE 802.1Qbg.

egress. Outbound or outgoing, referring to a protocol data unit (PDU) exiting a device. See also ingress.

encapsulation. The technique used by layered protocols in which a layer adds its own header information to the protocol data unit (PDU) from the layer above. As an example, in the Open Systems Interconnection (OSI) Reference Model, a PDU can contain a header for Layer 1 (L1), followed by a header for Layer 2 (L2), followed by a header for the Layer 3 (L3), followed by a header for the transport layer (Transmission Control Protocol (TCP), followed by data for the higher layers.

encryption. The process of encoding information in an attempt to make it secure from unauthorized access, particularly during transmission. The reverse of this process is known as decryption. Two main encryption schemes are in common use:

- Private (symmetrical) key: Using a private encryption key known to both the sender and the receiver of the information.
- Public (asymmetrical) key: Using a public key to encrypt and a private key to decrypt.

See also Data Encryption Standard (DES).

end-of-row switch. A chassis-based switch in a rack or cabinet at either end of the server row in a data center that connects to hundreds of servers in that row. Each cabinet in the row has cabling connecting 48 (or more) servers to the end-of-row switch. An end-of-row switch typically has redundant supervisor engines, power supplies, and overall better high availability characteristics than a Top-of-Rack (ToR) switch.

An end-of-row switch extends Layer 1 (L1) cabling topology from the switch to each rack, resulting in a smaller Layer 2 (L2) footprint and fewer Spanning Tree Protocol (STP) nodes in the topology.

Enhanced Transmission Selection (ETS). A protocol for assigning bandwidth to frame priorities. Defined in IEEE 802.1Qaz.

equal-cost multipath (ECMP). A forwarding mechanism for routing traffic along multiple paths of equal cost that ensures load balancing. The link-state routing protocols that use a cost-based metric such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) explicitly allow ECMP routing.

Encapsulating Security Payload (ESP). An Internet Protocol Security (IPsec) protocol that ensures confidentiality by encrypting IP packets. An encryption algorithm combines the data in a packet with a key to transform the packet into an encrypted form. At the destination, the packet is decrypted it using the same algorithm. ESP also

ensures the integrity of a packet using a hash message authentication code (HMAC). ESP also supports an authentication scheme like that used in Authentication Header (AH), or can be used in conjunction with AH.

Ethernet. A specification for a LAN technology at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model based on packetized transmissions between physical ports over a variety of electrical and optical media. Ethernet can transport several upper-layer protocols, the most popular of which is Transmission Control Protocol/Internet Protocol (TCP/IP). Ethernet standards are maintained by the IEEE 802.3 committee.

Ethernet uses a bus topology and CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to resolve contention when two devices try to access the network at exactly the same time. Transmission speeds range from 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet Linear Protection Switching (ELPS). A type of Automatic Protection Switching (APS) that specifies these techniques:

- Linear 1+1 (One-plus-One) operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities
- Linear 1:1 (One-to-One) operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source

Defined by ITU-T G.8032.

Ethernet Local Management Interface (E-LMI). An Operation, Administration, and Maintenance (OAM) protocol for communications between two User-to-Network Interface (UNI) instances. E-LMI provides both UNI and Ethernet Virtual Connection (EVC) status information to customer edge devices. This information enables automatic configuration of customer edge operation based on the configuration. Defined by Metro Ethernet Forum (MEF) 16.

Ethernet Ring Protection Switching (ERPS). A type of Automatic Protection Switching (APS) that protects traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Operation, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding database (FDB). Defined by ITU-T G.8032.

Ethernet to the First Mile (EFM). A set of extensions to the 802.3 MAC and MAC sub layer. EFM describes technologies and the physical layer specifications for subscriber access, including remote failure detection, remote loop back, and link monitoring. Defined by IEEE 802.3ah.

Ethernet Virtual Connection (EVC). An association of two or more instances of a User-to-Network Interface (UNI). There are three types of EVC:

- In a point-to-point EVC, exactly two UNIs are associated with one another.
- In a multipoint EVC, two or more UNIs are associated with one another.
- In a rooted-multipoint EVC, one or more of the UNIs must be designated as root and each of the other UNIs must be designated as a leaf. If root, the UNI can send service frames to all other points in the EVC; if leaf, the UNI can send and receive service frames to and from root only.

Explicit Route Object (ERO). An extension to Resource Reservation Protocol (RSVP) that allows a path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.

Exterior Gateway Protocol (EGP). An interdomain protocol such as Border Gateway Protocol (BGP) used to exchange network reachability information between autonomous system (AS) instances. Contrast with Interior Gateway Protocol (IGP).

F

FEC-to-NHLFE (FTN) map. In Multi-Protocol Label Switching (MPLS), a mapping from the forwarding equivalence class (FEC) of incoming packets to the corresponding Next Hop Label Forwarding Entry (NHLFE).

filtering. The process of determining whether to forward a frame or packet through a port. The simplest form of filtering is to not forward frames out the same port on which they were received. A network administrator can configure filtering manually or a device can be "self-learning" and record the source addresses of devices on each segment of a network in a filtering database.

Filtering behavior is sometimes referred to as "drop, flood, or forward":

- If the switch determines that the destination MAC is on the same port, it does not forward the frame, dropping it.
- If the switch determines that the destination MAC is on a different port, it forwards the frame on that port.
- If the switch does not know where to send the frame (or if it is multicast or broadcast), the frame is flooded out all ports (except the port it was received on).

filtering database. A data structure in a switch that maps addresses to ports, addresses to VLANs, and/or ports to VLANs. A switch learns the location of hosts by recording the source MAC address-port number association for each frame received at an incoming port. All future transmissions destined to a MAC address in the filtering database are only directed to the port associated with that MAC address unless the transmission originated on that port.

A switch can also be configured and act as several independent switches by creating VLAN associations to switch ports.

flapping. Condition of network instability when a route is announced and then withdrawn repeatedly, usually as the result of an intermittently failing link. Also called route flapping.

flooding. Forwarding a frame onto all ports except the port upon which it arrived. In Open Shortest Path First (OSPF), distributing and synchronizing the link-state database (LSDB) between routers.

flow control. Any mechanism that prevents a source from sending faster than the destination is capable of receiving.

Forward Error Correction (FEC). A system of error control that allows the receiver to correct some errors without having to request a re-transmission of data.

forwarding. Finding the output port to which a frame needs to go, and relaying the frame to that port.

forwarding equivalence class (FEC). A set of packets with similar characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same Multi-Protocol Label Switching (MPLS) label. FECs are defined by the Label Distribution Protocol (LDP). FECs are also represented in other label distribution protocols.

Forwarding Information Base (FIB). A data structure used to find the interface to which to forward a packet. The FIB contains the minimum amount of information required to make a forwarding decision for a particular packet, such as destination prefix and nexthop. The FIB is an abbreviated form of the information in the Routing Information Base (RIB).

Also called forwarding table.

frame. A protocol data unit (PDU) at Layer 2 (L2) with addressing and protocol control information. A frame contains a header field and a trailer field that "frame" the user data. (Some control frames contain no data.)

See also packet.

G

GARP Multicast Registration Protocol (GMRP). A Generic Attribute Registration Protocol (GARP) application that allows switches to exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups. See also Multiple MAC Registration Protocol (MMRP).

GARP VLAN Registration Protocol (GVRP). A Generic Attribute Registration Protocol (GARP) application that provides VLAN registration services. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs. Defined by 802.1Q. See also Multiple VLAN Registration Protocol (MVRP).

gateway. A device that understands and converts between two different networking models. Since Transmission Control Protocol/Internet Protocol (TCP/IP) has become the dominant model, gateways are not used much at this time.

See also default gateway.

Generic Attribute Registration Protocol (GARP). A generic framework for devices to register attributes, such as VLAN identifiers and multicast group membership. See also Multiple Registration Protocol (MRP).

generic routing encapsulation (GRE). A tunneling protocol that encapsulates Layer 3 (L3) packets inside IP packets. GRE provides a virtual point-to-point link over an IP network. GRE is completely insecure, but provides a fast and simple way to access a remote network.

graceful restart. A process that allows a router whose control plane is restarting to continue forwarding traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router. Also called nonstop forwarding.

gratuitous ARP. Broadcast request for a router's own IP address to check whether that address is being used by another node. Used to detect IP address duplication.

H

hash message authentication code (HMAC). A method of calculating a message authentication code (MAC) using a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-2, can be used to calculate an HMAC.

header. The portion of a protocol data unit (PDU) that contains control information for the message such as destination address, source address, input sequence number, the type of message, and priority level.

hello packet. A multicast packet that is used by protocols for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.

high availability. The ability of a system or component to limit or avoid network disruption when a component fails. High availability provides both hardware and software methods to minimize downtime and improve the performance of a network.

hold down. A state that a route is placed into so that devices will neither advertise the route nor accept advertisements about the route for a specific length of time (the hold down period). A hold down is used to flush bad information about a route from all devices in a network. A route is placed into hold down when a link in that route fails.

hop. A single link between two computer systems that a protocol data unit (PDU) must cross on its way to its destination. See also hop count.

hop count. The number of links that must be crossed to get from a source to a destination. A protocol data unit (PDU) might pass over many hops to reach its destination. If it must pass between five computers, it is said to have taken four hops to reach its destination. Hop count is often used as a metric for evaluating a route in distance-vector routing. Routing Information Protocol (RIP) uses hop count as its sole metric.

host. A computer connected to a network that is assigned a Layer 3 (L3) address and that provides an access point to that network. Similar to a node, except that host usually implies a computer system, whereas node generally applies to any networked device such as a router or switch.

hypervisor. A thin operating system designed solely to provide virtualization. A hypervisor drives physical hardware, executes virtual machine (VM) instances, and dynamically shares the underlying hardware with the associated virtual hardware. A hypervisor does not serve as a general-purpose operating system, but instead provides the platform on which VMs can run.

I

I-SID (Service Instance Identifier). A field in an I-TAG that defines the service instance to which the Provider Backbone Bridging (PBB) frame is mapped.

I-TAG. Field in the Provider Backbone Bridging (PBB) header that carries the I-SID (Service Instance Identifier) associated with the frame.

Incoming Label Map (ILM). In Multi-Protocol Label Switching (MPLS), a mapping from incoming labels to corresponding Next Hop Label Forwarding Entry (NHLFE).

ingress. Inbound or incoming, referring to a protocol data unit (PDU) entering a device. See also egress.

Institute of Electrical and Electronics Engineers (IEEE). A coordinating body for computing and communications standards. The IEEE mainly covers Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model. (Pronounced “eye-triple-ee”.) See http://www.ieee.org.

interface. The point at which a connection is made between two devices. An interface describes the logical and physical connections and usually means the same thing as the term port.

Interior Gateway Protocol (IGP). An intradomain protocol used to exchange network reachability and routing information among devices within an autonomous system (AS), such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP). Contrast with Exterior Gateway Protocol (EGP).

Intermediate System to Intermediate System (IS-IS). An Interior Gateway Protocol (IGP) that floods link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. A Routing Information Base (RIB) is calculated from the database by constructing a shortest path tree (SPT).

Like Open Shortest Path First (OSPF), IS-IS uses the Dijkstra algorithm to find the best path through a network. Packets are then forwarded, based on the computed ideal path, through the network to the destination.

Defined by International Organization for Standardization (ISO) 10589.

internal spanning tree (IST). A special type of multiple spanning-tree instance (MSTI) that runs in an multiple spanning-tree (MST) region. An IST connects all the switches in the MST region and appears as a subtree in the common and internal spanning tree (CIST) that encompasses the entire switched domain.

An IST is identified by the number zero (0) and exists on all ports; you cannot delete the IST. By default, all VLANs are assigned to the IST. The IST is the only spanning tree instance that sends and receives bridge protocol data unit (BPDU) messages.

Any other spanning tree instance within an MST region is called a multiple spanning-tree instance (MSTI).

International Organization for Standardization (ISO). An international standards body that establishes global standards for communications and information exchange. Voting members are designated standards bodies of participating nations; American National Standards Institute (ANSI) is the U.S. member of the ISO. The Open Systems Interconnection (OSI) Reference Model is one of the ISO's most widely accepted recommendations.

Sometimes mistakenly referred to as the "International Standards Organization". Because "International Organization for Standardization" has different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), the founders gave it the short form ISO. ISO is derived from the Greek *isos*, meaning "equal".

For more, see http://www.iso.org/iso/home.html.

International Telecommunication Union (ITU). An international organization that develops standards for telecommunications. Formerly known as the CCITT. See http://www.itu.int.

Internet. The world's largest computer network, serving universities, commercial interests, government agencies, and private individuals. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, and Internet computers and devices run many different operating systems.

No government agency, single person, or corporate entity controls the Internet. All decisions on methods and standards are made by standards groups based on input from users.

See also Internet Engineering Task Force (IETF); Request for Comments (RFC).

Internet Control Message Protocol (ICMP). An Internet Protocol (IP) that provides management and control functions. Routers send ICMP messages to respond to undeliverable datagrams by placing an ICMP message in an IP datagram and then sending the datagram back to the original source. ICMP is also used by the ping (packet internet groper) command and enables a host to discover addresses of operating routers on the subnet. Defined in RFC 792.

IPv6 makes greater use of ICMP (ICMPv6 defined in RFC 4443) than IPv4, including neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect.

Internet Engineering Task Force (IETF). An international community of network designers, operators, vendors, and researchers that develops Request for Comments (RFC) documents that define protocols and specifications for the Internet. The IETF mainly covers Layer 2 (L2) and Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. See http://www.ietf.org.

Internet Group Management Protocol (IGMP). An IPv4 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3376.

IGMP enables receivers to register that they want to receive a particular multicast transmission, but does not route multicast traffic from the source to receivers. That task is left to a multicast routing protocol, such as Protocol Independent Multicast (PIM).

See also Multicast Listener Discovery (MLD), multicast group, (S,G).

Internet Key Exchange (IKE or IKEv2). An Internet Protocol Security (IPsec) protocol used to set up a security association (SA) by negotiating keys in secret. IKE builds upon Internet Security Association and Key Management Protocol (ISAKMP) using X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

The IKE protocol runs in two phases. The first phase establishes a ISAKMP SA which is used in the second phase to negotiate and set up the IPsec SAs.

Internet Protocol (IP). A Layer 3 (L3) protocol that provides connectionless delivery of data across heterogeneous physical networks. IP provides features for addressing, type-of-service, fragmentation and reassembly, and security. Defined by RFCs 791 and 1349.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP is best effort and provides no guarantees of reliability, so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level—that is left to protocols a layer above, such as Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec). A protocol suite for securing IP communications by authenticating and encrypting packets during a communication session. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main wire-level protocols used by IPsec. Before either AH or ESP can be used, however, the two devices must share a public key through Internet Key Exchange (IKE or IKEv2).

RFC 2401 specifies the base architecture for IPsec compliant systems. RFCs 2402, 2406, and 2407 provide more details about IPsec.

Internet Security Association and Key Management Protocol (ISAKMP). A framework for authentication and key exchange with actual authenticated keying material provided either by manual configuration with pre-shared keys or Internet Key Exchange (IKE or IKEv2). See also Internet Protocol Security (IPsec).

IP address. A unique number that identifies a device on an Internet Protocol (IP) network. IP addresses have two formats:

- An IPv4 address is 32 bits and is usually written in dotted decimal notation as four decimal numbers separated by periods. For example, 192.168.50.4 is an IPv4 address.
- An IPv6 address is 128 bits and is written in a hexadecimal notation of eight 16-bit parts separated by colons. For example, FE80:0000:0000:0000:0202:B3FF:FE1E:8329 is an IPv6 address. In the double colon address format, consecutive colons (“::”) represent successive 16-bit blocks that contain zeros: FE80::0202:B3FF:FE1E:8329. While a much larger address space is a feature, IPv6 also has other features such as multicast support, jumbograms (packets up to 4 GB in size), and stateless host auto-configuration.

Table 13-102 compares the IPv4 and IPv6 address formats.

Table 13-102: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Address space	128-bits = 3.4 x 1038 (340 unidecillion)	32-bits = 4.3 x 109 (4.2 billion)
Field separator	colon (:)	period (.)

Table 13-102: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Notation	hexadecimal	decimal
Example	db8:0:0:1	0.23.2.3

Each IP address contains a network part, an optional subnetwork part, and a host part. The network and subnetwork parts together are used for routing, while the host part is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork parts from the IP address. Classless Interdomain Routing (CIDR) provides a way to represent IP addresses and subnet masks.

IP addresses are difficult to remember, so people tend to refer to computers by their domain names instead.

IPv6 Provider Edge (6PE). A protocol that enables IPv6 domains to communicate with each other over an Multi-Protocol Label Switching (MPLS) IPv4 core network. V6PE routers are “dual stack” and run both IPv4 and IPv6. Multiprotocol Border Gateway Protocol (BGP) (MP-BGP) in the IPv4 network is used to exchange IPv6 reachability information along with a label for each IPv6 prefix announced. Defined in RFC 4798.

Also called V6PE.

K

keepalive message. A message sent between devices when no data traffic has been detected for a given period of time. This communication verifies that the virtual and physical connection between the devices is still active.

kernel. The part of an operating system that performs basic functions such as allocating hardware resources.

KVM (Kernel-based Virtual Machine). A virtualization infrastructure for the Linux kernel that turns it into a hypervisor. KVM requires a processor with hardware virtualization technology extensions. By itself, KVM does not perform any emulation. Instead, KVM exposes an interface with which a user space host can then set up guest virtual machine (VM) instances.On Linux, QEMU (Quick EMUlator) is one such user space host.

L

Label Distribution Protocol (LDP). A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to create label-switched path (LSP) instances through a network by mapping network layer routing information directly to data-link layer switched paths.

A label is a short fixed-length, locally-significant identifier that identifies a forwarding equivalence class (FEC).

LDP works with other routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) to create LSPs.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

label edge router (LER). A router that operates at the edge of an Multi-Protocol Label Switching (MPLS) network and acts as the entry and exit points for the network.

When forwarding IP packets into an MPLS domain, an LER makes the initial path selection, add the appropriate labels to the packet, and forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using

normal IP forwarding rules. (Under penultimate hop popping (PHP), the popping function might be performed by an label switch router (LSR) directly connected to the LER.)

Also called an edge LSR.

label switch router (LSR). A Multi-Protocol Label Switching (MPLS) router located in the middle of a MPLS network. When an LSR receives a packet, it uses the label included in the packet header to determine the next hop on the label-switched path (LSP) and find a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is forwarded.

Also called transit router.

label-switched path (LSP). A sequence of routers that cooperatively perform Multi-Protocol Label Switching (MPLS) operations for a packet stream. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same device.

latency. Delay in the transmission through a network from source to destination. See also line rate, wire speed.

Layer 1 (L1). The physical layer in the Open Systems Interconnection (OSI) Reference Model that conveys the bit stream through electrical impulse, light waves, or radio signals through the network. L1 represents the basic network hardware and specifies the type of medium used for transmission and the network topology.

Layer 2 (L2). The data link layer in the Open Systems Interconnection (OSI) Reference Model that provides reliable transit of data across a physical link between two directly connected devices. L2 refers to physical addressing, network topology, line discipline, error notification, sequenced delivery of frames, and flow control.

L2 transfers data between network entities by splitting data into frames to send on Layer 1 (L1) and receiving acknowledgment frames. The data link layer performs error checking and retransmits frames not received correctly. In general, the data link layer controls the flow of information across the link, providing an error-free virtual channel to Layer 3 (L3).

The data-link layer has two sublayers:

- logical link control (LLC)
- Media Access Control (MAC)

Also called link layer.

Layer 3 (L3). The network layer in the Open Systems Interconnection (OSI) Reference Model that routes packets of data from source to destination across a network. L3 provides network-wide communication, including global addressing, lifetime control, fragmentation, and reassembly. Internet Protocol (IP) is an example.

Layer 4 (L4). The transport layer in the Open Systems Interconnection (OSI) Reference Model that provides logical communication between processes running on different hosts. L4 manages the end-to-end delivery of payload from a source to a destination within and between networks while maintaining the quality of service. Transmission Control Protocol (TCP) is an example.

Lightweight Directory Access Protocol (LDAP). A protocol used to locate organizations, individuals, and other resources in a network. Defined in RFC 4511. See also authentication, authorization, and accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

line rate. Total number of physically transferred bits per second, including useful data and protocol overhead, over a communication link. For example, if the line rate of a link is 10 Gbps, the link transmits 10 gigabits of data every second over its physical interface. Contrast with throughput. See also latency, wire speed.

link. Communication path between two neighbor nodes.

link aggregation. A method for using multiple parallel links between a pair of devices as if they were a single higher-performance channel. The aggregated interface is viewed as a single link to each device. Spanning Tree Protocol (STP) also views it as one interface. Link aggregation can also be used to increase availability so that when there is a failure in one physical link, the remaining links stay up, and there is no disruption. Defined by IEEE 802.1AX.

Also called link aggregation group (LAG), LAG bundle, and EtherChannel. See also Link Aggregation Control Protocol (LACP), Multi-Chassis Link Aggregation (MC-LAG).

Link Aggregation Control Protocol (LACP). Mechanism for exchanging port and system information to create and maintain link aggregation groups.

link cost. An arbitrary number configured on an Open Shortest Path First (OSPF) interface which is used in shortest path first calculations.

Link Layer Discovery Protocol (LLDP). A mechanism for the devices on a network to advertise their identity, capabilities, and neighbors to each other. Defined by IEEE 802.1AB.

link state. Information about a link and link cost to neighboring routers.

link-state advertisement (LSA). An Open Shortest Path First (OSPF) protocol data unit (PDU) to share information on the operating state of a link, link cost, and other OSPF neighbor information. LSAs are used by the receiving routers to update their Routing Information Base (RIB)s.

link-state database (LSDB). The data structure on a router that contains all routing knowledge in a link-state network. An LSDB stores all link-state advertisement (LSA) instances produced by a link-state routing protocol such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS). Each router runs shortest path first (SPF) algorithm against this database to locate the best network path to each destination in the network.

link-state routing. A routing technique used by Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) where each router shares information with other routers by flooding information about itself to every reachable router in the area. Link-state protocols use characteristics of the route such as speed and cost to determine the best path. Link-state information is transmitted only when something has changed in the network.

Every router constructs a map of the connectivity of the network, determining the interconnections between all routers. As a router receives an advertisement, it stores this information in a link-state database (LSDB). Each router then independently calculates the best next hop from it to every possible destination in the network using the shortest path first (SPF) algorithm to build a shortest path tree (SPT) with itself as the center of that tree. The shortest path to each reachable destination within the network is found by traversing the tree. The collection of best next hops forms the router's Routing Information Base (RIB).

Link-state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of more computing cycles and more traffic compared to distance-vector routing.

See also Dijkstra algorithm.

Linktrace Message (LTM). A Connectivity Fault Management (CFM) protocol data unit (PDU) initiated by a Maintenance association End Point (MEP) to trace a path to a target MAC address, forwarded from Maintenance domain Intermediate Point (MIP) to MIP, up to the point at which the LTM reaches its target MEP.

Linux. A Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the kernel, the central part of the operating system that manages system services. Many people use the name “Linux” to refer to the complete operating system package which is called a Linux distribution which is made up of a collection of software based around the Linux kernel.

Linux has since been ported to more computer hardware platforms than any other operating system and is available for a wide variety of systems from small embedded systems up to supercomputers. In particular, networking devices such as switches and routers almost universally run some Linux distribution.

As an open operating system, Linux is developed collaboratively, meaning no one organization is solely responsible for its development or ongoing support. Companies participating in the Linux community share research and development costs with their partners and competitors.

Local Area Network (LAN). A group of computers and devices connected by a communications channel, capable of sharing resources among several users. LANs are based on a small physical area such as a building, floor, or department. LANs can connect to a wide area network (WAN). Ethernet is the most popular LAN technology.

logical link control (LLC). The higher sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The LLC sublayer provides the interface for Layer 3 (L3) and handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. See also Media Access Control (MAC).

loopback. A troubleshooting test in which a signal is transmitted from a source to a destination and then back to the source again so that the signal can be measured and evaluated.

M

MAC address. A permanent, unique serial number that uniquely identifies a network device among all other network devices in the world. MAC addresses are 12-digit numbers, 48 bits in length. MAC addresses are usually written as six groups of two hexadecimal digits, separated by hyphens (“-”) or colons (“:”):

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Each pair of hexadecimal digits represents one byte of the 6-byte (48-bit) address.

An example of a MAC address is 68:A3:C4:3B:8D:24:

- The first three parts (68:A3:C4) identify the manufacturer (Liteon Technologies)
- The second three parts (3B:8D:24) is the serial number assigned by the manufacturer

At Layer 2 (L2), other devices use MAC addresses to locate specific ports in a network, and to create and update a Routing Information Base (RIB). A MAC address maps to an IP address through the Address Resolution Protocol (ARP).

Also called physical address, Ethernet address, or hardware address.

MAC-in-MAC. See Provider Backbone Bridging (PBB).

Maintenance Association (MA). In Connectivity Fault Management (CFM), a set of Maintenance association End Point (MEP) instances, each configured with the same MAID (Maintenance Association Identifier) and Maintenance Domain (MD) Level, established to verify the integrity of a single service instance.

Maintenance association End Point (MEP). A Connectivity Fault Management (CFM) entity at the edge of a Maintenance Domain (MD) that confines CFM messages within the domain via the MD level. MEPs periodically transmit and receive Continuity Check Message (CCM) instances from other MEPs within the domain. MEPs are either “Up” (toward the switch) or “Down” (toward the wire).

Maintenance Domain (MD). In Connectivity Fault Management (CFM), the network or the part of the network for which faults in connectivity can be managed.

Maintenance domain Intermediate Point (MIP). A Connectivity Fault Management (CFM) entity that catalogs and forwards information received from Maintenance association End Point (MEP) instances. MIPs are passive points that respond only to CFM Linktrace Message (LTM) and loopback messages.

Management Information Base (MIB). A specification of objects used by Simple Network Management Protocol (SNMP) to monitor or change network settings. MIBs provides a logical naming scheme for resources on a network. A MIB contains information about a device such as settings, usage statistics, performance data, or physical properties (such as temperature or fan speed). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches. Standard MIBs are defined by the IETF.

Maximum Transmission Unit (MTU). The maximum number of bytes in a packet or frame. For Ethernet, the default MTU is 1500 bytes (data payload), but each media has different sizes. The Ethernet MTU is defined in RFC 894.

Media Access Control (MAC). The lower sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multiple-access network that uses a shared medium such as Ethernet. The MAC sublayer is the interface between the logical link control (LLC) sublayer and Layer 1 (L1).

mesh. A physical or logical network topology in which devices have many redundant interconnections. A full mesh is when all devices in a network have a connection to all other devices, a partial mesh is when some devices have a connection to all other devices.

Metro Ethernet Forum (MEF). A defining body for Carrier Ethernet with many participating organizations including service providers, and network hardware and software manufacturers. The MEF's mission is to accelerate the worldwide adoption of carrier-class Ethernet networks and services. For more, see http://metroethernetforum.org/.

Multi-Chassis Link Aggregation (MC-LAG). A technique that extends the link aggregation concept. At either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. Defined by IEEE 802.1AX.

Also called MLAG and Distributed Resilient Network Interconnect (DRNI).

Multi-Protocol Label Switching (MPLS). A method for forwarding packets through a network. MPLS operates between the traditional definitions of Layer 2 (L2) and Layer 3 (L3).

In a traditional IP network, each router performs an IP lookup to determine a next hop based on its routing table, and forwards the packet to that next hop. Every router in the path repeats this process, making its own independent routing decisions, until the final destination is reached.

In an MPLS network, the first device does a routing lookup, but instead of finding a next hop, it finds the final destination router and finds a pre-determined path from the source to the destination. The router applies a "label" based on this information. Other routers in the path use the label to route the traffic without needing to perform any additional IP lookups.

At each incoming (ingress) point of the network, packets are assigned a label by a label edge router (LER). Packets are forwarded along an label-switched path (LSP) where each label switch router (LSR) makes forwarding decisions based on the label information. At each hop, an LSR swaps the existing label for a new label that tells the next hop how to forward the packet. At the outgoing (egress) point, an LER removes the label, and forwards the packet to its destination via IP routing.

MPLS enables these applications: Virtual Private Network (VPN), traffic engineering (TE), and Quality of Service (QoS).

See also Label Distribution Protocol (LDP), Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Multi-Protocol Label Switching - Transport Profile (MPLS-TP). A subset of Multi-Protocol Label Switching (MPLS) with extensions that address transport network requirements. The extensions provide the same QoS, protection and restoration, and Operation, Administration, and Maintenance (OAM) as in SONET/SDH. In MPLS-TP, some of the MPLS functions are turned off, such as penultimate hop popping (PHP), label-switched path (LSP) merge, and equal-cost multipath (ECMP).

The use of a control plane protocol is optional in MPLS-TP. The control plane can set up an LSP automatically across a packet-switched network domain. However, some network operators might prefer to configure the LSPs statically without using an IP or routing protocol.

multicast. The process of a single host sending messages to a selected group of receivers. See also broadcast, unicast.

multicast group. A collection of hosts receiving packets from a host that is transmitting multicast packets. Only hosts that need to hear a particular multicast declare that requirement. A multicast group restricts traffic to just those paths between the sources and destinations associated with the multicast address. Membership is dynamic; when a host joins a group, it starts receiving the datastream, and when a host leaves a group, it stops receiving the datastream. When there are no more members, the group simply ceases to exist.

See also GARP Multicast Registration Protocol (GMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multiple MAC Registration Protocol (MMRP), (S,G).

Multicast Listener Discovery (MLD). An IPv6 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3810.

See also Internet Group Management Protocol (IGMP), multicast group, (S,G).

Multiple MAC Registration Protocol (MMRP). A protocol that manages multicast group MAC addresses. In addition, MMRP improves the convergence time of GARP Multicast Registration Protocol (GMRP). Defined by 802.1ak.

Multiple Registration Protocol (MRP). A generic registration framework with protocols, procedures, and managed objects for switches to register attributes with other switches in a LAN. Defined by 802.1ak. MRP replaces Generic Attribute Registration Protocol (GARP)

Multiple Spanning Tree Protocol (MSTP). An enhancement to the Rapid Spanning Tree Protocol (RSTP) where a separate spanning tree for can be configured for a VLAN group. Each VLAN group belongs to a multiple spanning-tree instance (MSTI). Several MSTIs can run in an multiple spanning-tree (MST) region, with each region interconnected in a common and internal spanning tree (CIST).

MSTP is backward compatible with both RSTP and Spanning Tree Protocol (STP).

Originally defined in IEEE 802.1s and later merged into 802.1Q.

multiple spanning-tree (MST) region. A collection of interconnected switches that have the same Multiple Spanning Tree Protocol (MSTP) configuration which includes region name, revision number, and VLAN-to-instance map. Each MST region can contain multiple instances of spanning trees. The network administrator must properly configure participating switches throughout the region. All regions are bound together using a common and internal spanning tree (CIST), which creates a loop-free topology across regions. An MST region appears as a single switch to spanning tree configurations outside the region.

multiple spanning-tree instance (MSTI). A group of VLANs in a spanning-tree instance managed by Multiple Spanning Tree Protocol (MSTP) within an multiple spanning-tree (MST) region. Within each MST region, MSTP maintains multiple spanning-tree instances. Each instance has a spanning-tree topology independent of other

spanning-tree instances. An MSTI provides a fully connected active topology for frames belonging to a VLAN. You can assign a VLAN to only one spanning-tree instance at a time.

An internal spanning tree (IST) is a special type of MTSI.

Multiple VLAN Registration Protocol (MVRP). A protocol that manages registration of VLANs, tracking which routers are members of which VLANs and which router interfaces are in which VLAN. MVRP removes routers and interfaces from the VLAN information when they become unavailable. MVRP improves the convergence time of GARP VLAN Registration Protocol (GVRP). Defined by 802.1ak.

N

name resolution. The process of translating an IP address to a name that is easily remembered by a person. In a TCP/IP environment, a name such as www.example.com is translated into its IP equivalent by the Domain Name Service (DNS).

neighbor. An adjacent system reachable by traversing a single subnetwork; an immediately adjacent device. Also called peer. See also adjacency.

Neighbor Discovery Protocol (NDP). An IPv6 protocol that nodes on the same link use to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4.

NETCONF (Network Configuration Protocol). A mechanism to install, manipulate, and delete the configuration of network devices. The operations, notifications, and the database contents supported by a particular NETCONF server are extensible, and defined with a modeling language called YANG. The database is used to store YANG data structures which represent the configuration of the device containing the NETCONF server. This configuration can be saved in non-volatile storage so the configuration can be restored upon reboot. Defined in RFC 6241.

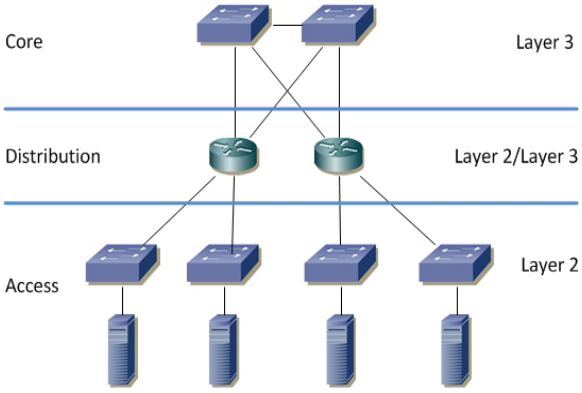
network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

A network can range from a peer-to-peer network connecting a small number of users in an office or department, to a Local Area Network (LAN) connecting many users, to a wide area network (WAN) connecting users on several networks spread over a wide geographic area.

network address translation (NAT). A method to use one set of IP addresses for an internal inetwork and a second set of addresses for the public Internet. This allows an organization to shield internal addresses from the public Internet. NAT is configured on the router at the border of an internal network and the Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the Internet and vice versa. Defined by RFC 1631.

network administrator. The person responsible for the day-to-day operation and management of a network.

network design model. A hierarchical model originally defined by Cisco that divides a network into three functional areas, or layers. This model optimizes network hardware and software to perform specific roles.



The roles that each layer performs are:

- The access layer provides local user access to the network
- The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing
- The core layer provides high-speed transport for the distribution layer

See also collapsed core.

Network Element (NE). Any device in a network such as a host, router, switch, or firewall that performs a service or function for the network.

Network Functions Virtualization (NFV). The ability to decouple network services from dedicated hardware devices to be hosted on a virtual machine (VM). Once the network services are under the control of a hypervisor, the services can be performed on standard x86 servers.

network layer. See Layer 3 (L3).

network segment. A portion of a computer network that is separated from the rest of the network by a device such as a router or switch. Each segment can contain one or more hosts.

Network Services Module (NSM). The base module in OcNOS that communicates with every OcNOS routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

Network Time Protocol (NTP). A protocol used to synchronize the system clocks of hosts on a network to Universal Coordinated Time (UTC). A device can update its clock automatically by configuring itself as an NTP client. Using NTP enables the device to record accurate times of events. Defined by RFC 5905.

Neutron. The networking component of OpenStack that provides “networking as a service” between virtual NICs managed by other OpenStack services.

Neutron provides a “plug-in” mechanism that lets network operators enable different technologies. It also lets tenants create multiple private networks and control their IP addressing. Organizations have control over security and compliance policies, Quality of Service (QoS), monitoring and troubleshooting, as well as the ability to deploy network services, such as a firewall, intrusion detection, and Virtual Private Network (VPN) instances.

next hop. The next device to which a protocol data unit (PDU) is sent on its way to its destination.

Next Hop Label Forwarding Entry (NHLFE). An Multi-Protocol Label Switching (MPLS) entry containing next hop information (interface and next hop address) and label manipulation instructions; it can also include label encoding, L2 encapsulation information, and other information to process packets in the associated stream.

node. An addressable device such as a host, router, or switch, attached to a network, that transmits and receives data.

north/south. The flow of traffic traversing between users and a data center (spanning-tree). Contrast with east/west.

northbound. An interface that allows a network component to communicate with a higher-level component. A northbound interface hides complex details of operations. Northbound flow can be thought of as going upward. In architectural diagrams, northbound interfaces are drawn at the top of the component. See also southbound.

Not-So-Stubby-Area (NSSA). An extension of a Open Shortest Path First (OSPF) stub area. OSPF uses an NSSA as a transit to send external routes to other areas or to domains that are not part of the OSPF autonomous system. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone. Defined by RFC 1587.

O

Open Network Foundation (ONF). A non-profit organization responsible for the development and standardization of a software architecture that supports Software-Defined Networking (SDN). ONF is also responsible for the commercialization and promotion of SDN as a concept and its underlying technologies. For more, see: https://www.opennetworking.org/.

Open Shortest Path First (OSPF). An Interior Gateway Protocol (IGP) based on link-state routing. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Defined in RFCs 2328 and RFC 5340.

OSPF advertises the states of local network links within an autonomous system (AS) and makes routing decisions based on the shortest path first (SPF) algorithm. Each OSPF router maintains an identical database describing the autonomous system's topology. From this database, a Routing Information Base (RIB) is calculated by constructing a shortest path tree (SPT).

OSPF features include least-cost routing, multipath routing, and load balancing. OSPF includes explicit support for Classless Interdomain Routing (CIDR) and the tagging of externally derived routing information.

OSPF version 2 supports IPv4 and OSPF version 3 supports IPv6.

OSPF divides an autonomous system into contiguous groups of networks called areas.

- In a standard area, intra-area routes, inter-area routes, and external routes (learned from other routing protocols such as RIP and BGP) are distributed. Inter-area routes and external routes are distributed as summary addresses.
- A backbone area is essentially a standard area which has been designated as the central point to which all other areas connect. A backbone area combines a set of independent areas into an AS and acts as a hub for inter-area transit traffic and routing information distribution. Each non-backbone area is directly connected to the backbone area.
- OSPF uses stub area instances and Not-So-Stubby-Area (NSSA) instances to limit distribution of inter-area routes and external routes.

See also area border router (ABR), autonomous system border router (ASBR).

Open Systems Interconnection (OSI) Reference Model. A conceptual model defined by the International Organization for Standardization (ISO) that organizes the computer-to-computer communications process into seven layers. Each layer provides services to the layer above and receives services from the layer below. Such a set of layers is called a protocol stack.

Layers seven through five manage end-to-end communications between the message source and destination, while layers one through four manage network access:

- Layer 4 (L4) ensures the end-to-end delivery from a source to a destination
- Layer 3 (L3) routes packets of data from source to destination across a network
- Layer 2 (L2) reliably transports data across the physical link between two directly connected nodes
- Layer 1 (L1) conveys the bit stream at the electrical and mechanical level

The OSI Reference Model is often compared to the more descriptive (versus prescriptive) Transmission Control Protocol/Internet Protocol (TCP/IP) model.

Open vSwitch (OVS). A software switch used in virtualized server environments that forwards traffic between different virtual machine (VM) instances on the same physical host and between VMs and the physical network. OVS enables network automation through programmatic extension, while still supporting standard management interfaces and protocols. For more, see http://openvswitch.org/.

OpenFlow. An open standard for forwarding plane operations that enables researchers to run experimental protocols. OpenFlow is developed, specified, and sponsored by the Open Network Foundation (ONF). OpenFlow provides a protocol that enables a controller to dynamically program internal flow-tables in devices. Network vendors have added OpenFlow features to routers and switches.

OpenStack. A cloud operating system that controls pools of compute, storage, and networking resources in a data center which users manage through a Web-based dashboard, command-line tools, or a RESTful API. See also Neutron.

Operation, Administration, and Maintenance (OAM). A set of Ethernet specifications that provide connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications are 802.3ah link-fault management (LFM) and 802.1ag Connectivity Fault Management (CFM).

P

packet. A protocol data unit (PDU) at Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. A packet contains source and destination addresses, user data, and control information such as the length of the packet, the header checksum, and flags indicating whether the packet has been fragmented. The user data in a packet is often referred to as the payload. The actual format of a packet depends on the protocol that creates the packet.

A packet sent through a connectionless protocol such as User Datagram Protocol (UDP) is sometimes called a datagram.

See also frame, packet switching.

packet switching. A data-transmission method that transmits information over one of several routes. Information is sent to the destination through the best route, determined by a routing algorithm.

A packet switched network breaks information to be transmitted into discrete packets. Related packets might not all follow the same path to their destination. Packet sequence numbers are used to reassemble the original message at the destination.

A packet-switched network is connectionless because each packet contains its destination address and does not require a dedicated path to reach that destination. Multiple users may transmit packets over the same connection at the same time, independent of one another.

The Internet is an example of a packet-switched network.

Contrast with circuit switching.

paravirtualized. A software component that is aware that it is running in a virtual machine (VM). For example, a paravirtualized virtual device driver runs in a VM that communicates with the underlying host OS. Typically, a paravirtualized driver is optimized to share queues, buffers, or other data items with the underlying host OS to improve throughput and reduce latency.

path computation element (PCE). An entity (component, application, or server) that can compute a network path or route based on a network graph and constraints (see RFC 4655).

path-vector routing. A routing technique that advertises a network as a destination address and a complete path to reach that destination. Each entry in the Routing Information Base (RIB) contains the destination network, the next router, and the path to reach the destination.

A path vector protocol guarantees loop-free paths by recording each hop the routing advertisement traverses through the network. A node can easily detect a loop by looking for its own node identifier in the path.

This technique is sometimes used in Bellman-Ford algorithm to avoid count-to-infinity problems.

Border Gateway Protocol (BGP) is an example of a prefix-based path-vector protocol where the Routing Information Base (RIB) maintains the autonomous systems to traverse to reach a destination.

peer. Immediately adjacent device with which a protocol relationship has been established. Also called neighbor.

penultimate hop popping (PHP). A technique where the outermost label of an Multi-Protocol Label Switching (MPLS) packet is removed by a label switch router (LSR) before the packet is passed to an adjacent label edge router (LER).

physical layer. See Layer 1 (L1).

ping (packet internet groper). A command used to test network connectivity by transmitting an Internet Control Message Protocol (ICMP) diagnostic packet to a specific node on the network, forcing the node to acknowledge that the packet reached the correct destination. If the node responds, the link is operating; if not, something is wrong.

The word ping is often used as a verb, as in “ping that workstation to see if it is alive.”

policing. Applying rate limits on bandwidth and burst size for traffic for a particular interface.

policy-based routing (PBR). Classifying packets to determine their forwarding path within a device. PBR is used to redirect traffic for analysis. Also called filter-based forwarding (FBF).

port. The point at which a communications circuit terminates on a network. A port can be logical, physical or both. Examples include:

- The physical interface between a device and a communications circuit, usually identified by a number or name.
- The logical interface between a TCP/IP applications and a communications facility which use well-known port numbers such as FTP: 20, HTTP: 80, and NFS: 2049.
- The logical interface between a process and a communications facility that allows more than one logical port to be associated with one physical port. For example, Ethernet uses multiple MAC addresses to distinguish between separate logical channels connecting two ports on the same physical transport network interface.

Also called interface.

Precision Time Protocol (PTP). A protocol that synchronizes clocks throughout a computer network. On a LAN, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. Defined by IEEE 1588v2.

Priority-based Flow Control (PFC). A flow control mechanism that can be set independently for each frame priority on full-duplex links. Defined by IEEE 802.1Qbb.

private VLAN (PVLAN). A switch with ports that cannot communicate with each other, but can access other networks. A PVLAN has at least one private port and a trunk port. All traffic received on a private port is forwarded out the trunk port. All traffic received on a trunk port is handled as normal switch traffic. No traffic communication occurs between the private ports.

protocol. A set of rules that end points in a network connection must follow when they communicate. A protocol includes data representation, data item ordering, message formats, message and response sequencing rules, block data transmission conventions, and timing requirements.

The Open Systems Interconnection (OSI) Reference Model and Transmission Control Protocol/Internet Protocol (TCP/IP) are both used as a model for many protocols. There are one or more protocols at each layer in the models that both ends of the connection must recognize and observe.

protocol data unit (PDU). A unit of data transmitted as a composite by a protocol.

In the Open Systems Interconnection (OSI) Reference Model, the actual name used for a PDU depends on the layer:

- Layer 4 (L4): segment
- Layer 3 (L3): packet
- Layer 2 (L2): frame
- Layer 1 (L1): stream, symbol stream, or bit stream

See also bridge protocol data unit (BPDU). Sometimes called datagram.

Protocol Independent Multicast (PIM). A method to determine the best paths for distributing a multicast transmission. PIM uses unicast routing tables (such as those used by Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)) and static routes to perform multicasting. Each host must be registered using IGMP to receive the transmission.

PIM has these variations:

- PIM dense mode (PIM-DM: RFC 3973) uses a push model. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats periodically.
- PIM sparse mode (PIM-SM: RFC 4601) uses a pull model. PIM-SM uses a shortest path tree (SPT) where sources forward multicast packets to a designated router which unicasts the packets to an assigned rendezvous point router, which then forwards the packets to members of multicast groups.
- PIM source-specific multicast (PIM-SSM: RFC 3569) uses PIM-SM functionality to create a SPT between the client and the source without using a rendezvous point.
- Bidirectional PIM (Bidir-PIM: RFC 5015) uses PIM-SM functionality to route traffic only along a bidirectional SPT that is rooted at the rendezvous point for a group.

protocol stack. The layers of software used in network communications.

Provider Backbone Bridge-Traffic Engineering (PBB-TE) . An extension to Provider Backbone Bridging (PBB) that removes features such as flooding, dynamically created forwarding tables, and spanning tree protocols. PBB-TE also covers Connectivity Fault Management (CFM) and Ethernet Linear Protection Switching (ELPS).

In PBB-TE, a network administrator configures the forwarding tables in the backbone switches with static routes to ensure that frames take predetermined paths within the network. Frames with destination MAC addresses not in a forwarding table are dropped. Broadcast frames are not supported and are also dropped by backbone switches.

Defined in IEEE 802.1Qay.

Provider Backbone Bridging (PBB). A technique to create Ethernet backbones for service access networks. Defined in IEEE 802.1ah, PBB extends Provider Bridging (PB) defined in 802.1ad in these ways:

- The 802.1ah header adds an I-SID (Service Instance Identifier) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at a backbone edge bridge (BEB). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (B-MAC) along with the customer source and destination MAC addresses (C-MAC). The B-MAC contains MAC addresses of the service provider's PBB edge switches. The 802.1ah format is sometimes called “MAC-in-MAC” because of this MAC address encapsulation. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Bridging (PB). A technique that enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate LANs, bridged LANs, or VLANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, so this limit could prevent a provider from having more than 4096 subscribers.

To overcome this limit, 802.1ad inserts an additional VLAN tag into a single 802.1Q Ethernet frame. Frames passing through the provider network are doubly tagged with:

- customer VLAN (C-VLAN) tag which identifies the customer network VLAN
- service VLAN (S-VLAN) tag which identifies the service provider network VLAN

With two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 VLANs.

The frame format for 802.1ad is also called Q-in-Q, double tagged, stacked VLANs, or VLAN stacking.

provider edge (PE). A device at the edge of an enterprise or service provider core network. A PE offers an initial, first level of network traffic aggregation for many customer edge (CE) devices.

pseudowire (PW). An emulation of a point-to-point connection over a packet-switching network. A pseudowire is a way to transport legacy services such as TDM over a packet-switched network:

- Structure-aware TDM circuit emulation service over packet-switched network (CESoPSN)
- Structure-agnostic TDM over packet (SAToP)

A pseudowire that both originates and terminates on the edge of a single packet-switched network (autonomous system or carrier network) is called a single-segment pseudowire (SS-PW). A pseudowire that extends through multiple autonomous systems or carrier networks is called a multi-segment pseudowire (MS-PW).

Q

Q-in-Q. See Provider Bridging (PB).

QEMU (Quick EMUlator). A hosted hypervisor that performs hardware virtualization. QEMU emulates CPUs through dynamic binary translation and provides a set of device models enabling it to run a variety of unmodified guest operating systems. QEMU also can be used together with KVM (Kernel-based Virtual Machine) to run virtual machines at near-native speed (requiring hardware virtualization extensions on x86 machines). QEMU can also be used purely for CPU emulation for user-level processes, allowing applications compiled for one architecture to be run on another.

Quality of Service (QoS). The ability to *guarantee* the delivery, control the bandwidth, set priorities for specific network traffic, and provide an appropriate level of security. QoS provides a level of predictability and control beyond the best effort delivery that a device provides by default.

See also Class of Service (CoS).

Quantized Congestion Notification (QCN). An end-to-end congestion management scheme for protocols capable of transmission rate limiting. Defined by IEEE 802.1Qau.

R

radio access network (RAN). The air interface and base station technology in a cellular network. In addition to the RAN, the entire cellular system includes the core network, which provides the backbone and services, as well as the cellphones.

Rapid Per-VLAN Spanning Tree Plus (RPVST+). A version of Cisco Per VLAN Spanning Tree Plus (PVST+) that uses the Rapid Spanning Tree Protocol (RSTP) state machine. PVST+ runs a spanning tree instance for each VLAN in the network. PVST+ is not scalable when there are many VLANs in a network. A compromise between RSTP and R-PVST+ is Multiple Spanning Tree Protocol (MSTP) which runs multiple instances of spanning tree that are independent of VLANs. MSTP maps a set of VLANs to each spanning tree instance.

Rapid Spanning Tree Protocol (RSTP). An enhancement to the Spanning Tree Protocol (STP) that re-configures quickly after a topology change. RSTP can verify if a port can change to a forwarding state safely without waiting for timers to start convergence. RSTP is not aware of VLANs and blocks ports at the physical level. Defined by IEEE 802.1D. See also Multiple Spanning Tree Protocol (MSTP).

Remote Authentication Dial In User Service (RADIUS). An authentication and accounting protocol to authenticate users and authorize their access to the requested system or service.

Defined in RFCs 2058, 2059, and 2865. See also authentication, authorization, and accounting (AAA), Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System Plus (TACACS+).

remote monitoring (RMON). A Management Information Base (MIB) specification that defines functions for remotely monitoring networked devices. The RMON specification provides many problem detection and reporting capabilities. Defined by RFC 2819.

Request for Comments (RFC). Proposals and standards that define protocols for communications over the Internet. RFCs are developed and published by the Internet Engineering Task Force (IETF).

Resource Reservation Protocol (RSVP). A signalling protocol for reserving resources across a network. RSVP is rarely used by itself, but Resource Reservation Protocol—Traffic Engineering (RSVP-TE) is widely used.

Resource Reservation Protocol—Traffic Engineering (RSVP-TE). RSVP with traffic engineering extensions, as defined by RFC 5101, that allows RSVP to establish label-switched path (LSP) instances in Multi-Protocol Label Switching (MPLS) networks, using Constrained Shortest Path First (CSPF), taking into consideration constraints such as available bandwidth and explicit hops. The LSPs might not agree with the route suggested by the Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

reverse path forwarding (RPF). An algorithm that checks the unicast Routing Information Base (RIB) to determine whether there is a shortest path back to the source address of an incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.

Rivest-Shamir-Adleman (RSA). A public key, or asymmetric, encryption scheme. The oretical background to RSA is that it is difficult to find the factors of a very large number that is the product of two prime numbers. RSA is considered very secure provided a sufficiently long key is used.

route. The path from source to destination through a network.

route flap damping. Method for minimizing instability caused by route flapping. The router stores a penalty value for each route. Each time the route flaps, the router increases this value. If the penalty for a route reaches a configured suppress value, the router does not include the route as a forwarding entry and does not advertise the route to peers.

route redistribution. One protocol learning routes from another protocol running on the same device. Also called redistribution or route leakage.

route reflection. A method of allowing iBGP routers to accept and propagate iBGP routes to their clients.

To avoid routing loops, Border Gateway Protocol (BGP) does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full mesh requirement becomes difficult to manage. To handle scaling problems, BGP uses route reflection and BGP confederations.

Route reflection allows you to designate one or more routers as route reflectors. BGP relaxes the re-advertising restriction on route reflectors, allowing them to accept and propagate iBGP routes to their clients.

route summarization. Consolidating multiple routes into a single route advertisement, in contrast to flat routing where a Routing Information Base (RIB) contains a unique entry for each route.

Classless Interdomain Routing (CIDR) is used to implement route summarization. All IP addresses in the route advertisement must have identical high-order bits.

Also called route aggregation. See also subnet mask.

router. A Layer 3 (L3) device that makes decisions about the paths over which network traffic will flow. Routers use dynamic routing protocols to learn about the network and to find the best route to forward packets toward their final destination:

1. Find a matching destination address in the Routing Information Base (RIB)
2. Find the MAC address for the packet from the Address Resolution Protocol (ARP) cache
3. Write the new MAC address in the IP packet
4. Send the packet on the port associated with the MAC address

routing. The process of finding a path to a destination to use to transmit a protocol data unit (PDU) over a network. Routing is usually controlled by a Routing Information Base (RIB) which defines where a PDU should go. Each router only needs to know where a PDU should be sent on its next hop, and does not know nor care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a PDU reaches its destination.

Routing Information Base (RIB). A data structure in a device that lists the routes to destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Network administrators can also add fixed routes to the RIB for static routing.

Also called a routing table. Contrast with Forwarding Information Base (FIB).

Routing Information Protocol (RIP). An Interior Gateway Protocol (IGP) that implements a distributed variant of the Bellman-Ford algorithm to provide distance-vector routing capabilities. RIP uses the hop count of a destination to detect the best path to route packets, but limits the maximum number of hops to 15 to prevent routing loops. RIP implements split horizon techniques. Defined in RFC 1058.

RIP is easy to configure and has low processing requirements. However, the hop count limit restricts the size of the network that RIP can support. Also, RIP can be slow to converge.

RIPv2 defined in RFC 2453 also supports subnet information, allowing Classless Interdomain Routing (CIDR).

RIPng (next generation), an extension of RIPv2 defined in RFC 2080, supports IPv6.

routing protocol. A set of processes, algorithms, and messages that are used to exchange routing information and populate the local Routing Information Base (RIB) with the best path between a source and destination.

The term “routing protocol” usually implies dynamic routing, where a device reports changes and shares information with other devices in the network. Each router starts with knowledge of only the devices to which it is directly attached. The routing protocol shares this information first with its immediate neighbors, and then throughout the network. This way, routers learn the topology of the network.

A primary benefit of dynamic routing protocols over static routing is that routers exchange information when there is a topology change. This exchange allows routers to automatically learn about new devices and networks and also to find alternate paths when there is a link failure in the current network.

Table 13-103 summarizes the characteristics of the dynamic routing protocols supported by OcNOS:

Table 13-103: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Algorithm	path-vector routing	distance-vector routing	link-state routing	link-state routing
Type	Exterior Gateway Protocol (EGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)
Classless Interdomain Routing (CIDR)	Yes	RIP v1: No RIP v2: Yes	Yes	Yes
Scalable	Yes	No	Yes	Yes
Speed of convergence	Moderate	Slow	Fast	Fast

Table 13-103: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Resource Use	High	Low	High	High
Configuration ease	Complex	Simple	Complex	Complex

routing table. See Routing Information Base (RIB).

S

S-TAG. See service VLAN (S-VLAN).

(S,G). A notation used in multicast that enumerates a shortest path tree (SPT) where:

- S is the IP address of the source
- G is the multicast group address that identifies the receivers

If the IP address of the source is 192.1.1.1, and the IP address of the multicast group is 224.1.1.1, the source group is written as (192.1.1.1, 224.1.1.1).

Secure Shell (SSH). A protocol that allows the opening of a secure, encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and other functions.

segment routing. A form of source routing where nodes and links are represented as segments. The path that a particular protocol data unit (PDU) needs to traverse is represented by one or more segments.

server. A system entity that provides a service to other entities called clients.

service VLAN (S-VLAN). In a Provider Bridging (PB) frame, a tag that identifies the service provider network VLAN. See also customer VLAN (C-VLAN). Also called an S-TAG or S-VID tag.

Shortest Path Bridging (SPB). A control plane protocol that combines an Ethernet data path with an Intermediate System to Intermediate System (IS-IS) link state protocol running between switches. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS link-state packets to discover and advertise the network topology and compute the shortest path tree (SPT) instances from all bridges in the SPB area. SPB only requires provisioning at the edge of the network. Defined by IEEE 802.1aq, with RFC 6329 describing the IS-IS extensions to support SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses a Provider Bridging (PB) (802.1ad) data path
- Shortest Path Bridging - MAC (SPBM) uses a Provider Backbone Bridging (PBB) (802.1ah) data path

shortest path first (SPF). Algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

shortest path tree (SPT). A Routing Information Base (RIB) formed by using the shortest path first (SPF) algorithm.

shortest-path routing. A routing algorithm in which paths to all network destinations are calculated. The shortest path is then determined by a cost assigned to each link.

signalling. The ability to transfer information within a network or between different networks.

Simple Network Management Protocol (SNMP). A standardized framework for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- SNMP manager: The system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports the data SNMP managers.
- Management Information Base (MIB): How SNMP exposes data as variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

SNMP uses User Datagram Protocol (UDP) to send and receive messages on the network.

Single Root I/O Virtualization (SR-IOV). A specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices:

- PFs are used to configure and manage the SR-IOV functionality
- VFs are lightweight and contain all the resources necessary for data movement but have a minimal set of configuration resources

SR-IOV enables network traffic to bypass the software switch layer of a virtualization stack. The I/O overhead in the software emulation layer is nearly the same as in nonvirtualized environments.

Software-Defined Networking (SDN). An approach to designing, building, and operating networks that decouples the control plane from the data plane. The control plane is centralized in the form of a controller system. Communication between the controller system and the network device uses a standard protocol such as OpenFlow or other agents. The controller system can consist of multiple, domain specific, clustered controllers. An SDN architecture usually includes APIs that developers use to control the underlying network. These APIs can be standards-based, or they can be vendor-specific.

source routing. A technique where the sender of a protocol data unit (PDU) can partially or completely specify the route that the PDU should take through the network. See also segment routing.

southbound. An interface that allows a network component to communicate with a lower-level component. A southbound interface breaks down the concepts into smaller technical details that are specifically geared toward the lower-layer component within the architecture. Southbound flow can be thought of as going downward. In architectural diagrams, southbound interfaces are drawn at the bottom of the component. See also northbound.

spanning tree algorithm. A technique that finds the best path between segments of a multilooped, mesh network. If multiple paths exist in the network, the spanning tree algorithm finds the most efficient path and limits the link between the two networks to this single active path. If this path fails because of a cable failure or other problem, the algorithm reconfigures the network to use another path.

From the point of view of an individual switch, a spanning tree has a root node and one path that connects all the other switches.

Spanning Tree Protocol (STP). A protocol that creates spanning trees within mesh networks of connected devices, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes. Defined by 802.1D.

STP devices exchange bridge protocol data unit (BPDU) messages. The spanning tree algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers can set up redundant links as backups in case active links fails. Automatic backup takes place without the pitfalls of bridge loops or the need to manually enable or disable backup links.

See also Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

split horizon. A technique where routes learned from an interface are not advertised on that same interface, preventing the router from seeing its own route updates.

In split horizon with poison reverse, routes learned from an interface are set as unreachable and advertised on that same interface which also prevents the router from seeing its own route updates.

stacked VLAN. See Provider Bridging (PB).

static address. An address permanently assigned to a device. Contrast with a dynamic address.

static routing. A method where a network administrator programs connecting paths between networks into a router. If a connection fails, the administrator must reprogram the router to use a new path. Static routes have precedence over routes chosen by dynamic routing protocols.

stub area. A type of Open Shortest Path First (OSPF) area where external routes are distributed as a single default route (address 0.0.0.0). Inter-area routes are distributed in a stub area as summary addresses.

In a *totally stubby area*, a single default route is distributed for all external *and* inter-area routes. Addresses from both other areas and external networks are distributed as the default route (address 0.0.0.0).

See also Not-So-Stubby-Area (NSSA).

subnet mask. A bit pattern that shows how an Internet address is divided into network, subnetwork, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

This is an example is this IPv4 address and subnet mask:

192.168.100.12 with subnet mask of 255.255.255.0

The first 24 bits of the address is the network address (192.168.100.0) and the last 8 bits are the hosts (12). The entire subnet spans the address range 192.168.100.0 to 192.168.100.255.

The addresses on a given subnet are always contiguous and can all be derived from the network address. Bit masks are always with respect to binary digits, so the number of IP addresses on a given subnet is always some power of two.

A mask gives the first address in the block (the network address) when ANDed with an address in the block.

Classless Interdomain Routing (CIDR) represents the equivalent of a subnet mask by adding a prefix length to an IP address that is the number of bits in the network portion. For example, the subnet mask above can be written as:

192.168.100.12/24

where 192.168.100.12 is the IP address and /24 is the number of bits in the subnet mask.

A subnet mask represents the same information as a prefix length, but predates the use of CIDR.

Also called address mask, network mask.

subnetwork. A group of related IP addresses that all begin with the same network portion and end with a unique portion identifying the host within the subnet.

Also called subnet. See also subnet mask.

subsequent address family identifier (SAFI). Number that further identifies an address family.

supernetting. The process of taking several discrete network addresses and advertising them as one route. For example, if an organization is using 192.10.1.0/24 to 192.10.254.0/24, instead of advertising 254 separate networks, the organization can advertise only the single route 192.10.0.0/16.

switch. A Layer 2 (L2) device that forwards frames based on a destination MAC address. A switch finds a destination address in its filtering database and transmits the frame on the port associated with the destination address. The filtering database is populated through a self-learning process, where each incoming frame is used to update the entries in the filtering database.

A switch that is VLAN-aware can also forward frames based on VLAN identifiers. A network administrator can configure this mapping manually or a switch can dynamically learn mappings via GARP VLAN Registration Protocol (GVRP).

Basic switch behavior is defined in IEEE 802.1D and 802.1Q.

See also bridge. Contrast with router.

Synchronous Ethernet (SyncE). SONET/SDH/PDH-based synchronization that is used to synchronize and send frequency information to devices on an Ethernet network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

T

telnet. A client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of purposes.

Terminal Access Controller Access Control System Plus (TACACS+). An authentication method that provides access control for networked devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting (AAA) services. (Usually pronounced like tack-axe.)

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

throughput. Average rate of successful delivery of data packets over a communication link. Throughput is measured in bits per second, data packets per second, or sometimes data packets per time slot. See also line rate, latency, wire speed.

time to live (TTL). A limit on how long a piece of information can exist before it should be discarded. TTL is a field in an IP header that is (usually) decremented by 1 for each hop through which the packet passes. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.

Top-of-Rack (ToR) switch. In a data center, an access layer switch that connects to servers installed in the same rack. A ToR switch is usually low profile (one or two rack units in height) with a low port count (typically 48 ports). All cabling for servers stays within the rack as relatively short cables from the servers to the switch. The switch connects

the rack to the data center network with one fiber uplink to a distribution layer switch. There is no need to run cabling between racks and each rack can be managed as a modular unit.

A ToR switch extends the Layer 2 (L2) topology from the aggregation switch to each individual rack resulting in a larger Layer 2 footprint.

See also end-of-row switch.

topology. The physical or logical layout of a network.

topology change notification (TCN). In Spanning Tree Protocol (STP), a bridge protocol data unit (BPDU) that a switch sends to signal a topology change.

traffic engineering (TE). The ability to control the path taken through a network based on a set of traffic parameters. Traffic engineering optimizes the performance of networks and their resources by balancing traffic load across links, routers, and switches in the network. See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Transmission Control Protocol (TCP). A Layer 4 (L4) protocol that works above Internet Protocol (IP) and provides reliable data delivery over connection-oriented links.

TCP splits the stream of data into packets with a sequence number, and sends the packets over an IP-based network. At the destination, TCP acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application. If TCP detects a missing, corrupted, or out of order packet, it requests it be resent from the source.

See also Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP).

Transmission Control Protocol/Internet Protocol (TCP/IP). A family of Internet protocols that describe how data should be formatted, addressed, transmitted, routed, and received to enable computers to communicate over a network.

The Open Systems Interconnection (OSI) Reference Model is a more prescriptive (versus descriptive) approach to network design. TCP/IP does not map cleanly to the OSI model because it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

TCP/IP is a widely published open standard and is supported by many vendors and is available on many different computers running many different operating systems. TCP/IP is separated from the network hardware and will run over Ethernet and other connections.

TCP/ IP also refers to the specific functionality at layers 4 and 3:

- Transmission Control Protocol (TCP) at Layer 4 (L4) splits a message into packets that are transmitted over the Internet and reassembles the packets into the original message at the destination
- Internet Protocol (IP) at Layer 3 (L3) addresses and routes each packet so that it gets to its destination

transport layer. See Layer 4 (L4).

tunneling. A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote VPN client have encrypted access to a private network.

type of service (ToS). A field in the IPv4 header used to differentiate packet flows. See also Differentiated Services (DiffServ).

type-length-value (TLV). A data structure used to encode optional information in a data communications protocol:

- Type: the kind of field that this part of the message represents

- Length: the size of the value field, usually in bytes
- Value: a variable-sized set of bytes that contains the data of the message

U

unicast. The process of a single host sending messages to one destination.See also broadcast, multicast.

User Datagram Protocol (UDP). A connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery and which requires other protocols to handle error processing and retransmission. Defined in RFC 768.

Multicast applications that deliver audio and video streams use UDP as their delivery mechanism because the acknowledgment and retransmission services offered by Transmission Control Protocol (TCP) are not needed and add too much overhead.

User-to-Network Interface (UNI). The physical interface/demarcation between a service provider and a subscriber, the service start or end point. There are two types of UNI:

- UNI-C: customer-side processes
- UNI-N: network-side processes

V

VirNOS. An IP Infusion product based on Network Functions Virtualization (NFV) that helps network operators deploy and manage networking services. Many core networking services, including switching, routing, load balancing and VPN can be performed by software either running directly on x86-64 servers or running as virtual machine (VM) instances instead of requiring expensive networking equipment. Therefore, organizations are migrating networking functions to standard, high-volume server environments and replacing dedicated network hardware with virtualization software that runs on commodity servers. Carriers, service providers, enterprises and network equipment manufacturers can run VirNOS as-is, on top of a standard server platform. IP Infusion customers can integrate VirNOS into their software offering and thereby add services and features quickly.

Virtual Ethernet Bridge (VEB). A virtual switch implemented in a virtualized server environment. A VEB mimics a traditional external Layer 2 (L2) switch for connecting to a virtual machine (VM). VEBs can communicate between VMs on a single physical server, or they can connect VMs to the external network. The most common implementations of VEBs are software-based vSwitches built into hypervisors.

Virtual Local Area Network (VLAN). A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs enable multiple bridged LANs to transparently share the same physical network link while maintaining isolation between networks. Traffic between VLANs is restricted to devices that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

VLANs make it easy to administer logical groups of hosts that can communicate as if they were on the same LAN.

Membership in a particular VLAN can be by port, MAC address, protocol, or subnet.

VLANs are configured as unique Layer 2 (L2) broadcast domains. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. VLANs span one or more ports on multiple devices and several VLANs can co-exist on a single physical switch. By default, each VLAN maintains its own filtering database containing MAC addresses learned from frames received on ports belonging to the VLAN.

IEEE 802.1Q provides for tagging Ethernet frames with VLAN identifiers. 802.1Q only supports up to 4094 VLANs, which is a scaling constraint for service providers.

virtual machine (VM). An operating system or application environment installed on emulated hardware and not physically installed on dedicated hardware. The virtual machine's guest operating system does not have to be modified to run in a virtualized environment. A VM behaves like a traditional, physical server and runs a traditional operating system such as Windows or Linux.

A hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources. The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other. For example, virtual machines can run Linux and Windows operating systems and share the same underlying physical host. An operating sysem is unaware that it is running in a VM.

See also paravirtualized, virtualization.

virtual port. A port on a vSwitch (Virtual Switch) where virtual Ethernet adapters or physical uplinks can be attached. During their creation, virtual switches are typically configured with a specific number of virtual ports.

virtual private LAN service (VPLS). Multipoint-to-multipoint Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone.

VPLS evolved as a logical extension of Virtual Private Wire Service (VPWS) based on RFC 4447.

VPLS can be defined as several instances of a virtual switch instance (VSI) that are interconnected to form a single logical bridge domain.

Virtual Private Network (VPN). A network service which uses encryption and tunneling to provide a subscriber with a secure private network that runs over the public network infrastructure.

Virtual Private Wire Service (VPWS). Point-to-point Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone. Also called Virtual Leased Line (VLL) or Ethernet over MPLS (EoMPLS).

virtual router (VR). A OcNOS proprietary abstraction where multiple distinct logical routers exist within a single device. Each virtual router executes separate instances of the routing protocol and network management software. A virtual router provides support for multiple Routing Information Base (RIB) instances and multiple Forwarding Information Base (FIB) instances per physical router. Each VR might consist of an Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or Routing Information Protocol (RIP) routing process, each with its own Routing Information Base (RIB) and Forwarding Information Base (FIB). Applications include segregating traffic dedicated to different customers, enterprise Virtual Private Network (VPN) users, or a specific traffic type such as streaming video.

Do not confuse a Virtual Router Redundancy Protocol (VRRP) virtual router with a OcNOS virtual router. They are two different things.

Virtual Router Redundancy Protocol (VRRP). A protocol that uses a *virtual router*, an abstract representation of multiple routers (master and backup routers) that act as a group. VRRP advertises a virtual router as the default gateway instead of one physical router. Two or more physical routers are configured, with only one doing the actual routing at any given time. If the current physical router that is routing on behalf of the virtual router fails, the other physical router automatically takes over. Defined by RFC 5798.

Do not confuse a VRRP virtual router with an OcNOS virtual router (VR). They are two different things.

Virtual Routing and Forwarding (VRF). A technology that allows multiple instances of a Routing Information Base (RIB) to co-exist within the same router at the same time. Multiple VRFs inside a virtual router (VR) logically subdivide the RIBs. Service providers can use VRF technology to create a separate Virtual Private Network (VPN) for each of their customers. Therefore, the technology is also called VPN routing and forwarding.

virtual switch instance (VSI). A mechanism for VLANs to pass packets to other VLANs without sending the packets through a router. With a VSI, the switch recognizes packet destinations that are local to the sending VLAN and bridges (switches) those packets. Only packets destined for another VLAN are routed.

A VSI is similar to the bridging defined in IEEE 802.1Q; a frame is switched, based on the destination MAC and membership in a Layer 2 (L2) VPN. A VSI floods unknown, broadcast, or multicast frames to all ports associated with the VSI.

virtualization. A technology that abstracts the physical characteristics of a machine, creating a logical version of it, including creating logical versions of entities such as operating systems and network resources. See also hypervisor, virtual machine (VM).

vNIC (Virtual Network Interface Card). Software that behaves like a Ethernet hardware adapter. It has a MAC address, and it sends and receives Ethernet frames.

VPN routing and forwarding. See Virtual Routing and Forwarding (VRF).

vSwitch (Virtual Switch). Software that behaves like a physical Ethernet switch. A vSwitch connects virtual machine (VM) instances in a virtual network at layer 2:

- Connects vNIC (Virtual Network Interface Card) instances from multiple VMs to virtual ports
- Connects physical network interface cards to virtual ports
- Uplinks to the physical network

A vSwitch maintains a MAC address table and routes traffic to specific ports, rather than repeating traffic on all ports. A vSwitch can include other features found in physical Ethernet switches, such as VLANs.

See also Open vSwitch (OVS).

W

weighted fair queuing (WFQ). Queue scheduling discipline where each queue has a weight and is assigned a different percentage of output port bandwidth. WFQ supports variable-length packets so that flows with larger packets are not allocated more bandwidth than flows with smaller packets.

WFQ classifies traffic as high- or low-bandwidth with low-bandwidth traffic getting priority and high-bandwidth traffic sharing what is left over. If traffic bursts ahead of the rate at which the interface can transmit, new high-bandwidth traffic is discarded after a congestive-messages threshold has been reached.

WFQ provides preferential treatment for higher priority traffic while preventing total starvation of lower priority traffic under sustained overload conditions.

weighted random early detection (WRED). Congestion avoidance mechanism which prevents an output queue from ever filling to capacity. WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

weighted round-robin queuing (WRR). Queue scheduling discipline that supports flows with significantly different bandwidth requirements. Each queue can be assigned a weight that is relative to other queues. WRR ensures that lower-priority queues are not denied access to buffer space and output port bandwidth. At least one packet is removed from each queue during each service round.

white box switch. In computer hardware, a white box is a server without a well-known brand name made from commonly available parts. White box switches are like white box servers, offering low cost without the brand name or tight integration of silicon and network software features.

Traditional black box switches are built with vertically integrated hardware and software. Some vendors use custom application-specific integrated circuit (ASIC) components to boost performance and add features, which adds to the cost. A white box switch decouples the software from the switching hardware. By decoupling software and hardware, customers have more flexibility and can potentially change software without changing hardware.

A white box switch runs a network operating system on generic x86 hardware with “merchant silicon” chipsets from manufacturers such as Broadcom, Centec, Intel, Marvell, and Mellanox. White box switches rely on an operating system such as Linux to integrate the Layer 2 (L2)/Layer 3 (L3) networking functions.

White box switches do not have the same complex features as black box switches because most interact with Software-Defined Networking (SDN) controllers to make forwarding and control plane decisions from a centralized point for all switches in the network. The SDN controller uses OpenFlow (or another southbound API) to program the forwarding table of the white box switches.

Some vendors sell a complete white box solution with the operating system already installed, while others supply just the “bare-metal” switch and you buy the operating system direct from the software vendor.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a Local Area Network (LAN) and that may use or provide public communication facilities.

wire speed. The ability of a device to achieve throughput equal to the maximum throughput of a communication standard.

Y

YANG. A data modeling language that specifies the syntax and semantics for NETCONF (Network Configuration Protocol) operations, notification events, and database content. YANG tools can automate behavior within the NETCONF protocol for clients and servers.

YANG can model both configuration and state data of network elements. YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints. YANG data definitions provide a strong set of features for extensibility and reuse. Defined in RFC 6020.

Z

ZebHA. An IP Infusion product that ensures a pre-agreed level of operational performance by minimizing system downtime. A ZebHA system operates redundant nodes that can provide continued service when a node fails. High availability does not mean that components will never fail, but it ensures that the system is available when the user needs it even if components fail. ZebHA provides:

- Simplex-Active or Active-Standby (1+1) control plane redundancy
- Reliable handling of operational, application, system and component failures;
- Strict Service Level Agreements (SLA) requirements of network operator customers

ZebHA supports protocol modules in Layer 2 (L2) and Layer 3 (L3).

There are two types of protocol recovery after a redundancy switchover: stateful switchover (SSO) and graceful restart.

ZebIC. An IP Infusion product that enables network equipment manufacturers to develop networking solutions based on leading silicon platforms. ZebIC allows manufacturers to deliver networking products built around this switching platform.

ZebIC enables developers to develop, integrate, and test a target platform while the actual hardware system is still under development. Pre-integrated with ZebOS-XP control plane platform, ZebIC:

- Separates hardware development from software development through the ZebOS abstraction layer.
- Isolates all of the hardware and operating system specific interactions into a small set of well-defined function calls for the control plane.

ZebM. An IP Infusion product that allows network equipment manufacturers to develop management functionality for their networking products. ZebM provides a software framework and APIs for building on-device management systems for network equipment. The ZebM framework contains these core components:

- CML (Central Management Layer), transaction-oriented middleware that connects configuration and operational data on all management interfaces within a network device. CML is used by any northbound management application to manage ZebOS-XP or any third-party control plane.
- SMI (Simple Management Interface), a series of southbound Interface modules to connect with OcNOS or any third party control plane protocol modules. SMI is the interface between the managed object and the CML.
- Model-driven northbound interface for automatic rendering of interfaces such as command-line interface (CLI) and NETCONF (Network Configuration Protocol).

ZebOS-XP. An IP Infusion product with Layer 2 (L2) and Layer 3 (L3) control plane software that allows network equipment manufacturers to rapidly add networking capabilities to communications products. ZebOS-XP is targeted at manufacturers who provide solutions in carrier transport, access, Carrier Ethernet, mobile backhaul, data center, and cloud networking, including solutions for enterprise private clouds, hybrid clouds, and public clouds

The ZebOS-XP networking protocol modules conform to leading Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Metro Ethernet Forum (MEF), and other industry standards.

SECTION 20 Master Command Index

Master Command Index

SECTION 21 Index

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W