OcNOS®

Open Compute
Network Operating System
for Optical Transport Networks
Version 1.0.3

OcNOS Configuration Guide

October 2020

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.

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')
  dot1x                           IEEE 802.1X Port-Based Access Control
  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 RIP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

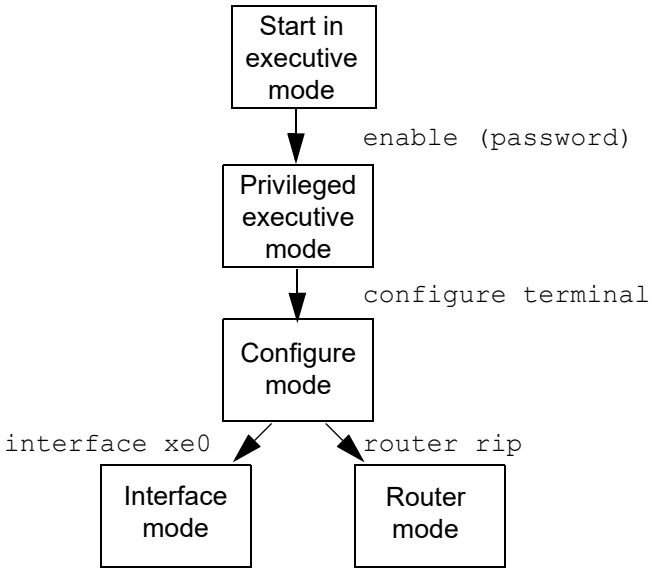


Figure P-1: Common command modes

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 starting `imish` and then moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
# ./imish
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router rip
(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, RIP, BGPv4, IS-IS
- Carrier 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.

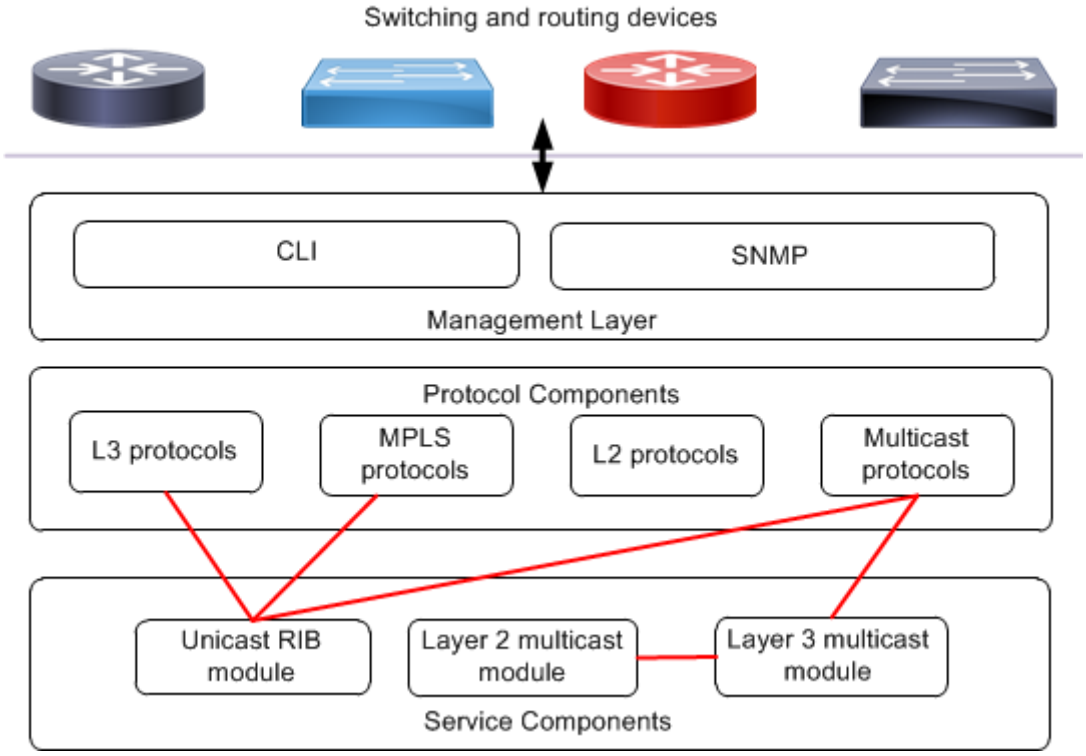


Figure 1-1: OcNOS high-level architecture

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
  - 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.

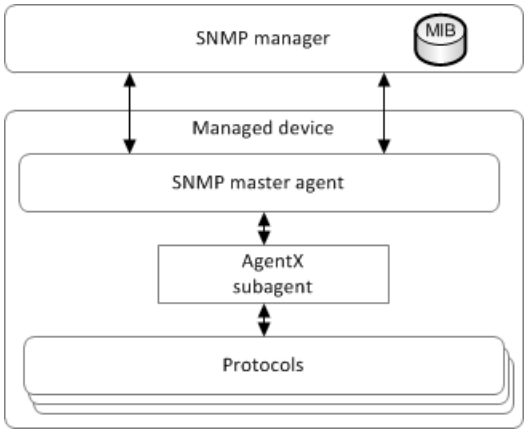


Figure 1-2: SNMP subagent

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
- Port Authentication (802.1x)
- Link Aggregation (802.1AX)

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.

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.

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.

Port Authentication (802.1x)

The OcNOS Layer 2 802.1x module provides port-based network access control (PNAC) for LAN devices. The IEEE 802.1x standard offers centralized control of user authentication and access.

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.

Layer 3 Protocols

OcNOS supports these IP protocols:

- Border Gateway Protocol
- Open Shortest Path First
- Routing Information Protocol

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

- Virtual Routing (VR) support
- 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, RIP, 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 1-3 shows how the Layer 3 protocols and the unicast RIB communicate.

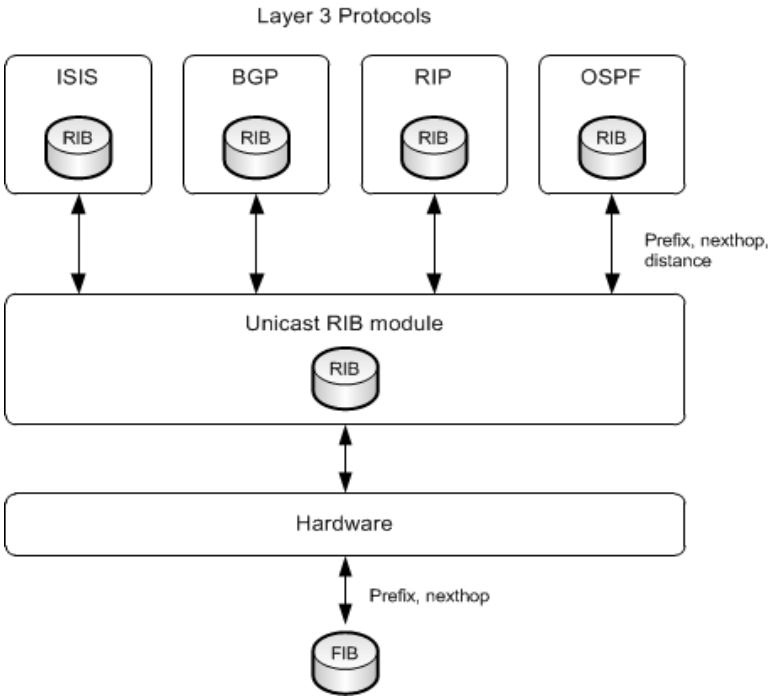


Figure 1-3: Protocol, unicast RIB, and kernel interaction

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, OSPF, and RIP
- 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.

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 VPNs
- BGP Graceful restart
- BGP Inter-Domain Routing (IDR):
  - Virtual Routing and 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

Routing Information Protocol

The Routing Information Protocol (RIP) version 2 is one of the most commonly used interior gateway protocols (IGP) for routing on internal IPv4 networks, and to a lesser extent, networks connected to the Internet. RIP employs a distributed variant of the Bellman-Ford algorithm to provide distance vector routing capabilities. RIP also supports subnet information, thus allowing Classless Inter-domain Routing (CIDR).

OcNOS RIP features include:

- Split horizons with poisoned reverse
- Triggered updates
- Full MIB support

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 1-4 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 installs them in the multicast FIB.

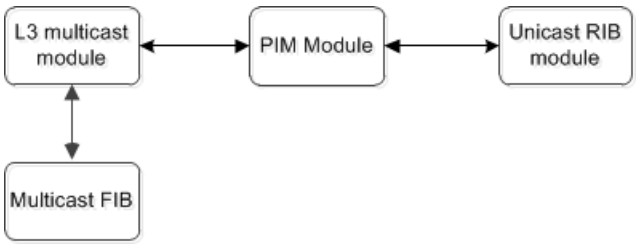


Figure 1-4: Layer 3 multicast architecture

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

System Management

The system management module supports these host protocols:

- Authentication, Authorization, and Accounting
- Dynamic Host Configuration Protocol Client
- Domain Name System
- Network Time Protocol
- 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.

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.

SECTION 2

System Management

System Management Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 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 configuration 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 configuration 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 configuration mode

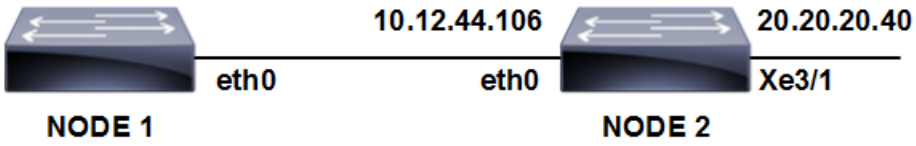
`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode

`(config-if)# no ip vrf forwarding management`	Remove in-band port from Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configuration 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 configuration 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 2 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 “user1” with password user12345 which will have default role as network-user.
`(config)#username user1 role network-operator password user12345`	Change the role for user1 to network-operator.
`(config)#username user2 role network-operator password user12345`	Create “user2” with role as network-operator.
`(config)#username user3 role network-admin password user12345`	Create “user3” with role as network-admin.
`(config)#username user4 role network-engineer password user12345`	Create “user4” with role as network-engineer.
`(config)#exit`	Exit configure mode.

Validation Commands

`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 3 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 3-5: 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 4 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 4-6: 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 configuration 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 configuration 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 configuration 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 configuration 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 4-7: SSH Key based Authentication sample topology

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 In-band (default VRF) and Out of band (management VRF). Installed keys are stored at ~/.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 command “ssh-keygen”.
2. Create username in OCNOS switch device (ssh server).
3. Install the public key of remote Linux ssh client in OCNOS device.
4. Display the installed key in OCNOS device using “show running-config”.
5. Login from remote Linux ssh client to OCNOS device without providing 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 AAAAB3NzaC1yc2EAAAADAQABAAABAQC 8XhFiGlZP6yY6qIWUkew884NvqXqMPS Ow3fQe5kgpXvX0SbcU15axI/ VHVgU2Y0/ ogAtRUlAk5soRrf5lZ2+rT0zNP37m+T m5HIEFKZZut0FffGSuXtPKbE+GGlQYH EzC8RSnqQuHlxrlve3lGbB1UUxuWhMz Jfgc2vZ78V2znd2zk4ygiN1jx1sE8UI 98WyIcwuq44tzuIaUYAICIfrQJXriQm l+QcJ9NER5O8rMS5D5NnTVh1nroqooz Y8i/ qMKfhCFMbysjiDMHU9GclNsNbIF/ DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ 4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain`	Install the public key of remote Linux client in ocnos device.
`#exit`	Exit configuration 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
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
OCNOS#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

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

Sample Use case:

Step 1 :

```
Login to remote machine linux desktop (ssh client) and generate the key pair
using the command “ssh-keygen”
[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
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
[bob@localhost .ssh]#
```

Step 2 :

```
Create username in OCNOS switch device (ssh server)
OCNOS(config)#username fred
Note : By default user role will be network-user
```

Step 3 :

```
Install the public key of remote Linux ssh client in OCNOS device.
OCNOS(config)#username fred sshkey
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
```

```
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
```

Step 4 :

```
Display the installed key in OCNOS device using "show running-config"
OCNOS#show running-config
<skipped other content>
username fred role network-user
username fred sshkey
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
```

Step 5 :

```
Login from remote Linux ssh client to OCNOS device without providing password
[bob@localhost .ssh]# ssh fred@10.10.26.186

OCNOS >en
OCNOS #
```

CHAPTER 5 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.

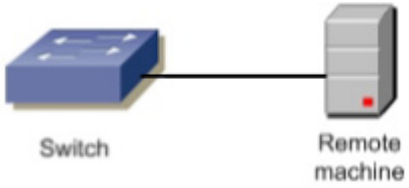


Figure 5-8: DHCP sample topology

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Enter 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 6 DHCP Snooping

Overview

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. It is a security feature that acts like a fire wall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in ‘man-in the middle’ or ‘Denial of Service’ attacks from malicious purpose. Similarly DHCP clients (rogue) can also cause ‘Denial of Service’ attacks by continuously requesting for IP addresses causing address depletion in the DHCP server.

The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from un-trusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and un-trusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about un-trusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from un-trusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Topology

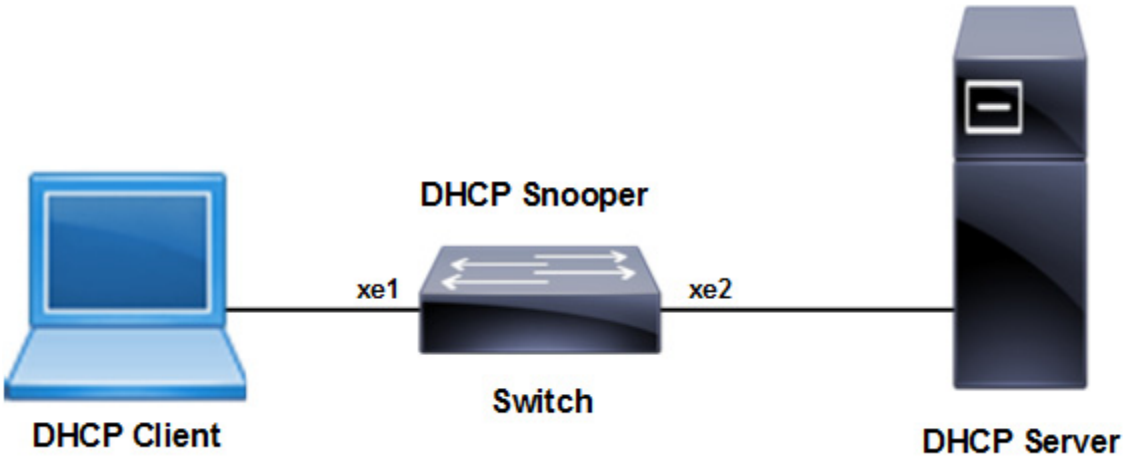


Figure 6-9: DHCP Snoop Topology

Configuration Guidelines

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP snooping globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the device acting as the DHCP server is configured and enabled.
- If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as un-trusted by entering the `no ip dhcp snooping trust interface` configuration command.

Procedures

The following subsections provide examples of how to enable and configure DHCP Snooping.

Enable DHCP Snooping Globally

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Create mstp or ieee vlan-bridge.
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge

Enable DHCP Snooping on a VLAN

`configure terminal`	Enter configure mode.
`(config)#vlan 2 bridge 1`	Configure a vlan for the bridge.
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2

Configuring the ports connected to DHCP server and DHCP client

`#configure terminal`	Enter the configure mode
`(config)#interface xe1`	Specify the interface xe1 to be configured, and Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `xe1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Specify interface `xe2` to be configured connected to server.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `xe2` with bridge-group `1`.

`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit the config mode.

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.

DHCP Snooping Operation

1. Configure DHCP server that is connected to DHCP Snooper through trusted port.
2. Request an ip address from the DHCP client connected through the un-trusted port.
3. DHCP client broadcast the DHCP DISCOVER message to the switch.
4. DHCP server responds to the DHCP DISCOVER message with DHCP offer message to the client.
5. Once the DHCP OFFER is received by the client, it sends an DHCP REQUEST to the server.
6. DHCP server validates the request from the client and sends DHCP ACK with the offered ip address to the client with the lease time.
7. DHCP Snooper creates an entry for the above operation into the binding table which includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.
8. DHCP Snooper clears the entry in the binding table once the client sends the DHCP RELEASE query.

Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device in question.

```
#show running-config ip dhcp snooping
!
!
```

```
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe2
 ip dhcp snooping trust
!
```

The `show ip dhcp snooping bridge 1` command displays the configured information about DHCP Snooping.

```
#show ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Rate limit(pps)                                       : 100
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2


DHCP snooping IP Source Guard is configured on the following Interface

Interface               Trusted
---------------         -------
xe2                     Yes
```

The `show ip dhcp snooping binding bridge 1` command displays the binding table entries associated with un-trusted interfaces.

```
#show ip dhcp snooping bridge 1

Bridge Group : 1
DHCP snooping is : Enabled
DHCP snooping option82 is : Disabled
Verification of hwaddr field is : Disabled
Rate limit(pps) : 100
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface  Trusted
--------   -------
  xe2        Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface               Source Guard
---------------         ------------
```

CHAPTER 7 DHCP Snooping IP Source Guard

Overview

IPSG is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. Use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

Enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

Topology

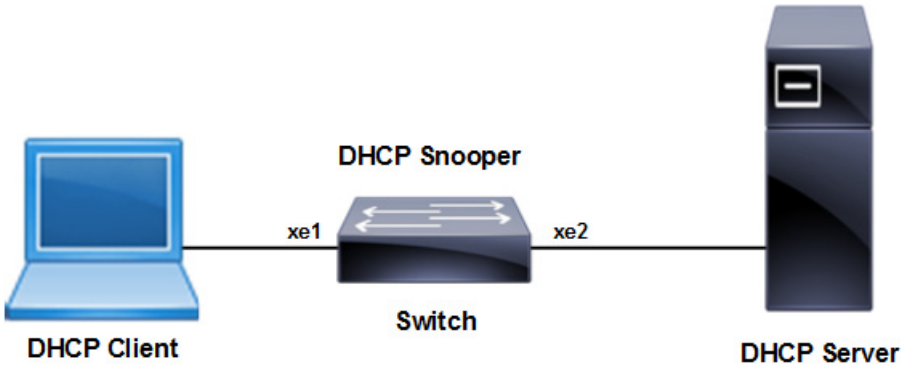


Figure 7-10: IP Source Guard Topology

Configuration

`#configure terminal`	Enter the configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)# ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)# ip dhcp snooping ratelimit 0` bridge 1	Configure DHCP snooping ratelimit. Default value is 100
`(config)# ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for vlan 2 for bridge 1
`(config)# ip dhcp snooping verify mac-address bridge 1`	Configure DHCP snooping verify mac-address
`(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 access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(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 access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe1	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe1	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv4 entries
(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv6 entries
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge:

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit (pps)                                      : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface               Trusted
---------------         -------
xe2                      Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
```

```
Interface                Source Guard
---------------          ------------
xe1                       Yes
```

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config-if)#exit`	Exit interface mode

Validation

Verify that static DHCP snooping entries are configured for the bridge:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                    : 1
Total number of dynamic IPV4 entries                   : 0
Total number of static IPV6 entries                    : 1
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   ---------------
0011.1111.2222       1.1.1.1           0          static          2      xe1
0022.2222.3333       3ffe::1           0          static          2      xe1
```

Verify that static IP DHCP snooping source guard entries are configured for the bridge:

```
#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries             : 1
Total number of static source IPV6 entries             : 1
MacAddress           IpAddress         Lease (sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      xe1
0022.2222.3333       3ffe::2           0          static          2      xe1
```

Configuring IP Source Guard on LAG Port

In this example, the LAG port (sa2) is created, then physical interfaces are added.

`#configure terminal`	Enter the configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)# ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)# ip dhcp snooping ratelimit 0 bridge 1`	Configure DHCP snooping ratelimit. Default value is 100
`(config)# ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for vlan 2 for bridge 1
`(config)# ip dhcp snooping verify mac-address bridge 1`	Configure DHCP snooping verify mac-address
`(config)#interface sa2`	Enter Interface Mode
`switchport`	Configure the interface as Layer 2
`bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#ip verify source dhcp-snooping-vlan`	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
`(config-if)#ip verify source access-group mode merge`	Merge IPSG policy with other ACL
`(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 access`	Set the Layer2 interface as Access. (It can be Trunk mode also)
`(config-if)#switchport access vlan 2`	Set the default VLAN for the interface
`(config-if)#ip dhcp snooping trust`	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
`(config-if)#exit`	Exit interface mode.
`(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 access`	Set the Layer2 interface as Access. (It can be Trunk mode also)
`(config-if)#switchport access vlan 2`	Set the default VLAN for the interface
`(config-if)#static-channel-group 2`	Configure Static Channel lag on the interface
`(config-if)#exit`	Exit interface mode
`(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 sa2`	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured

`(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 sa2`	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured
`(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface sa2 bridge 1`	Configure static IP source guard entry for ipv4 entries with lag interface
`(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface sa2 bridge 1`	Configure static IP source guard entry for ipv6 entries with lag interface
`(config)#exit`	Exit config mode
`#clear ip dhcp snooping binding bridge 1`	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge with the static LAG interface:

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit(pps)                                       : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface               Trusted
---------------         -------
Xe2                    Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface               Source Guard
---------------         ------------
sa2                     Yes
```

Verify that static DHCP snooping or source guard entries are configured for the bridge with the LAG interface:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                   : 1
Total number of dynamic IPV4 entries                  : 0
Total number of static IPV6 entries                   : 1
Total number of dynamic IPV6 entries                  : 0
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2
0022.2222.3333       3ffe::1           0          static          2      sa2

#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries            : 1
Total number of static source IPV6 entries            : 1
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2
0022.2222.3333       3ffe::2           0          static          2      sa2
```

CHAPTER 8 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

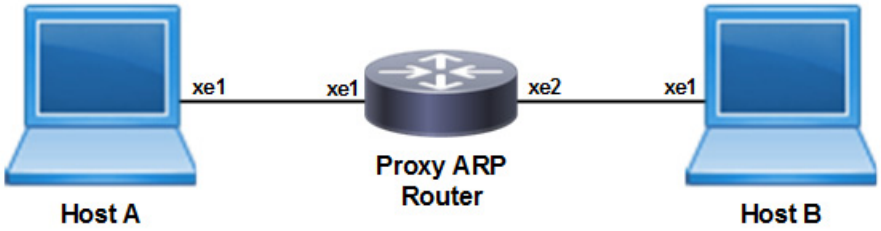


Figure 8-11: Sample topology

Configuration

Host A

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.1.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Proxy ARP Server

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.1/24`	Assign an IPv4 address to the interface

`(config-if)#ip proxy-arp`	Enable proxy ARP
`(config-if)#exit`	Exit interface mode
`(config-if)#interface xe2`	Enter interface mode
`(config-if)#ip address 20.20.1.1/24`	Assign an IPv4 address to the interface
`(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. The ARP table should have router's xe1 interface MAC address to reach Host B. Execute the command at Host A.

```
#show arp

Address                  HWaddress              Interface      Type
20.20.0.2                52:54:00:24:43:23       eth1          Dynamic
192.168.52.1             fe:54:00:0d:1e:dc       eth0          Dynamic
```

Local Proxy ARP Overview

The local proxy ARP feature enables local proxy support for ARP requests at the interface level. The router answers all ARP requests on the 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.

Local proxy ARP 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

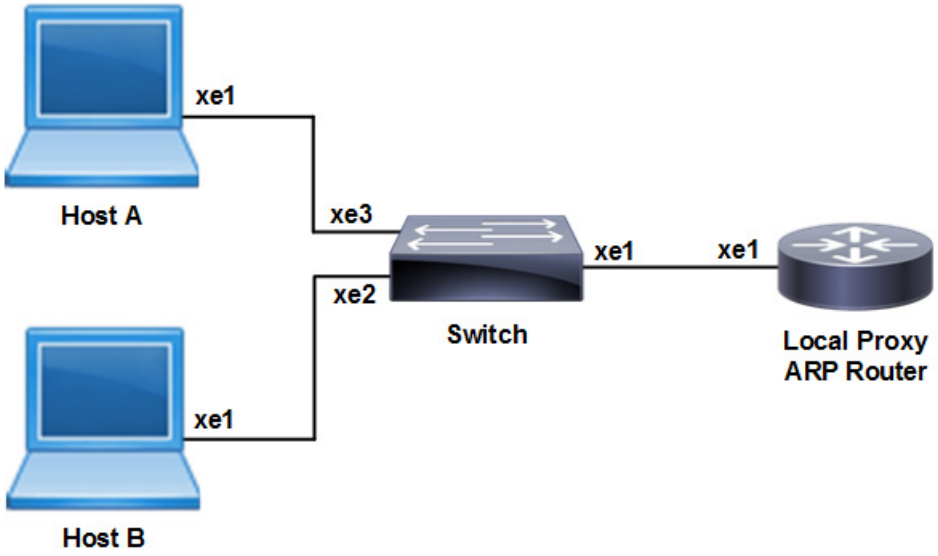


Figure 8-12: Sample topology

Configuration

Host A

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.3/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Switch Private VLAN

`#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 VLAN database mode
`(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 primary VLAN
`(config-vlan)#private-vlan 101 isolated bridge 1`	Configure VLAN 101 as isolated VLAN

(config-vlan)#private-vlan 100 association add 101 bridge 1	Associate secondary VLAN 101 to primary VLAN 100
(config-vlan)#exit	Exit VLAN database mode
(config)#interface xe1	Enter interface mode
(config-if)#switchport	Configure xe1 as a Layer 2 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	Make the interface 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	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 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	Make the interface 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	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 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	Make the interface 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

Router Local Proxy ARP

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.3/24	Assign an IPv4 address to the interface
(config-if)#ip local-proxy-arp	Enable local proxy ARP
(config)#end	Exit interface and configure mode

Validation

The show arp command on hosts shows the arp table entries to reach different subnets. Ping Host B from 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.
```

CHAPTER 9 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

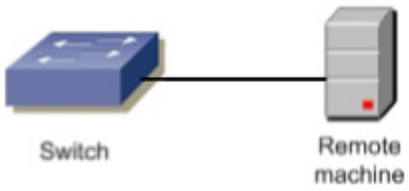


Figure 9-13: DNS sample topology

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

By default, NTP 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. 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 clock synchronization has actually happened, there will be an asterisk “*” symbol along with the interface when you give the `show ntp peers` command.

Topology

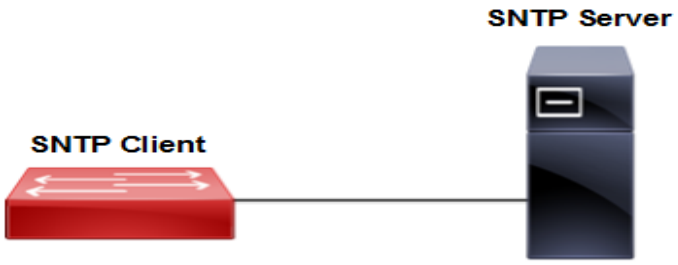


Figure 10-14: SNTP Client and Server

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 11 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 11-15: 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 11-1:

Table 11-1: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14

Table 11-1: 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 11-1.

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 11-1.

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 configuration 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 12 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 12-16: 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 10.16.19.2 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 10.16.19.2 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 10.12.30.86 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 10.12.30.86 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.

```
OcNOS#show radius-server vrf management
        VRF: management
Global RADIUS shared secret: ********
timeout value: 5

Total number of servers:3

Following RADIUS servers are configured:

               10.12.17.11:
                 available for authentication on port:60000
                 available for accounting on port:60000
                 timeout:6
                 RADIUS shared secret:********

               10.12.30.86:
                 available for authentication on port:1045
                 available for accounting on port:1813

               10.16.19.2:
                 available for authentication on port:1812
                 available for accounting on port:1813
                 RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:

               100.0.0.1:
                 available for authentication on port:60000
                 available for accounting on port:60000
                 RADIUS shared secret:********

               Radius-Server-1:
                 available for authentication on port:60000
                 available for accounting on port:60000
```

```
                  RADIUS shared secret:********
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********
```



```
                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:
```

```
                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server vrf management groups
        VRF: management

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf all groups
        VRF: management

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

        VRF: default

        group radius:
                server: all configured radius servers
```

```
        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server groups
        VRF: default

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf management groups rad1
        VRF: management

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf all groups rad1
        VRF: management

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********
```

```
                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********


        VRF: default

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server groups rad1
        VRF: default

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

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

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
```

```
                  RADIUS shared secret:********

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

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
```

```
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

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

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

                VRF: default
  default: group radius
  console: local

#show aaa authentication
                VRF: default
  default: group radius
  console: local

#show aaa groups vrf management
                VRF: management
radius
rad1

rad1

#show aaa groups vrf all
                VRF: management
radius
rad1

                VRF: default
radius
rad1

#show aaa groups
                VRF: default
radius
rad1


#show running-config radius
radius-server login host 100.0.0.1 vrf management key 7 wawyanb123 auth-port 600
00 acct-port 60000
radius-server login host Radius-Server-1 vrf management key 7 wawyanb123 auth-po
rt 60000 acct-port 60000
```

```
radius-server login host Radius-Server-1  key 7 wawyanb123 auth-port 60000 acct-
port 60000
radius-server login host 100.0.0.1 key 7 wawyanb123 auth-port 60000 acct-port 6
000

#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 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

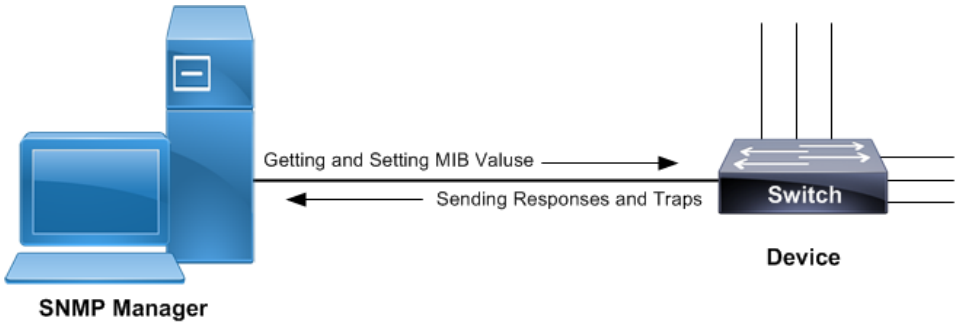


Figure 13-17: SNMP sample topology

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

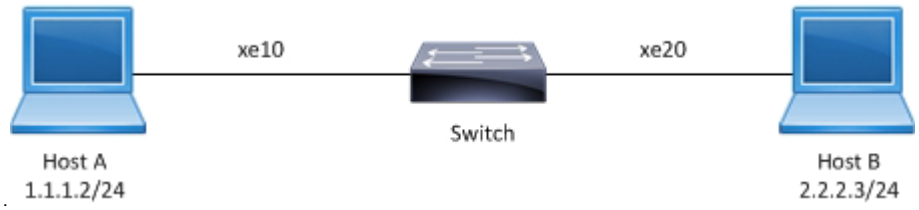


Figure 14-18: ACL sample topology

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

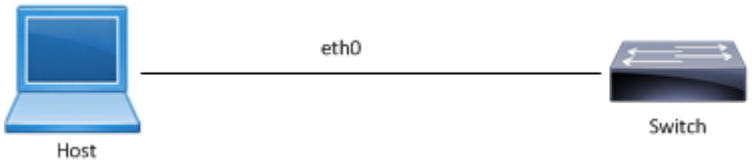


Figure 14-19: Management ACL Sample Topology

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 14-20: ARP ACL Sample Topology

ARP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge4`	Enter interface mode.
`(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 is the feature to be used to provide this basic level security for the management applications accessible through In-band interfaces.

Note: Refer to command reference section for limitation, default behavior, and not supported features.

Topology

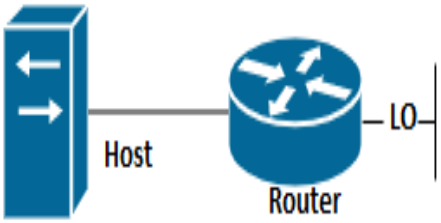


Figure 14-21: ACL Loopback Topology

Loopback ACL Configuration

`#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

Use the commands below to validate ACL loopback.

```
OcNOS#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

OcNOS#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:

OcNOS#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 VTY

•When a telnet or ssh connection is made the OcNOS associates this connection with a virtual terminal (VTY) line. ACL over vty feature provides security for management features associated with vty.

Note: Refer to command reference section for limitation, default behavior, and not supported features.

Topology

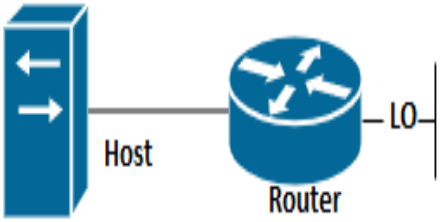


Figure 14-22: ACL VTY Topology

VTY ACL Configuration

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

Validation

```
OcNOS#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
OcNOS#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
OcNOS#sh running-config ac
access-list  aclmgr
OcNOS#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 LAG with RTAG7 Hashing

Overview

Traffic can be load balanced within an LACP trunk group and within an ECMP in a controlled manner using the RTAG7 hashing algorithm.

Topology

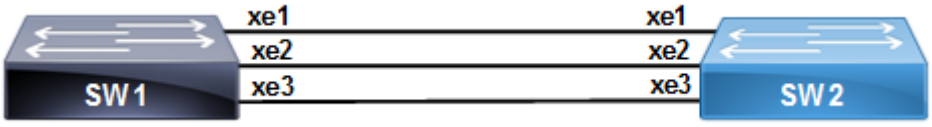


Figure 15-23: LACP with RTAG7 Configuration

Dynamic LAG with RTAG7

SW1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS.
`(config)#load-balance rtag7`	Enable load-balance for rtag7 globally.
`(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan`	Enabling load-balance rtag7 for l2 with all options.
`(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id`	Enabling load-balance rtag7 for ipv4 with all options.
`(config)#interface po1`	Enter into port channel interface po1.
`(config-if)#switchport`	Configure po1 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 all`	Allow all the VLANs on the xe1 interface.
`(config-if)#port-channel load-balance rtag7`	Enable rtag7 load-balancing method.
`(config-if)#exit`	Exit the po1 interface mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 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 all`	Allow all the VLANs on the xe1 interface.

(config-if)#channel-group 1 mode active	Make port as part of port channel
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel..
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe3 interface mode.

SW2

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANS.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Configure po1 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 all	Allow all the VLANs on the po1 interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 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 all	Allow all the VLANs on the xe1 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 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 all	Allow all the VLANs on the xe2 interface.

(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.

Validation

```
SW1#show etherchannel summary
Aggregator po1 100010
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5061) sync: 1
Link: xe2 (5062) sync: 1
Link: xe3 (5063) sync: 1

SW2#show etherchannel summary
Aggregator po1 7
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5013) sync: 1
Link: xe2 (5014) sync: 1
Link: xe3 (5015) sync: 1

SW1#show etherchannel detail
Aggregator po1 100001
Aggregator Type: Layer2
 Mac address: 3c:2c:99:28:52:1e
 Admin Key: 0001 - Oper Key 0001
  Actor LAG ID- 0x8000,3c-2c-99-7a-b2-e0,0x0001
  Receive link count: 3 - Transmit link count: 3
  Individual: 0 - Ready: 1
 Partner LAG ID- 0x8000,00-18-23-30-20-ce,0x0001
  Link: xe1 (5061) sync: 1
  Link: xe2 (5062) sync: 1
  Link: xe3 (5063) sync: 1
Collector max delay: 5
```

Static LAG with RTAG7

SW1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS
`(config)#load-balance rtag7`	Enable load-balance for rtag7 globally.
`(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan`	Enabling load-balance rtag7 for l2 with all options.
`(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id`	Enabling load-balance rtag7 for ipv4 with all options .
`(config)#interface sa1`	Enter into port channel interface sa1.
`(config-if)#switchport`	Configuresa1 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 all`	Allow all the VLANs on the sa1 interface.
`(config-if)#port-channel load-balance rtag7`	Enable rtag7 load-balancing method.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 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 all`	Allow all the VLANs on the xe1 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 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 all`	Allow all the VLANs on the xe2 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 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 all`	Allow all the VLANs on the xe3 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe3 interface mode.

SW2

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS.
`(config)#interface sa1`	Enter interface mode
`(config-if)#switchport`	Configure sa1 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 all`	Allow all the VLANs on the sa1 interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 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 all`	Allow all the VLANs on the xe1 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 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 all`	Allow all the VLANs on the xe2 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 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 all`	Allow all the VLANs on the xe3 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe3 interface mode.

Validation

```
SW1#show static-channel-group
 Static Aggregator: sa1
 Member Status
  xe1          up
  xe2          up
  xe3          up
SW1#
```

```
#show running-config interface sa1
!
interface sa1
load-interval 30
ip address 14.4.1.2/24
mtu 1600
port-channel load-balance rtag7
port-channel min-links 4
ip ospf network point-to-point
ip ospf cost 1000
```

CHAPTER 16 Port Breakout Configuration

This chapter contains an overview of splitting single 100G port to 4x10G ports.

Overview

Port Breakout system enables numerous 100GbE ports to be broken out into 4x10GbE, 4x25GbE, 2x50GbE ports through a secure, highly reliable breakout cabling solution. Today's large-scale virtualized datacenter networks require a mix of 10Gb, 25Gb, 40Gb and 100Gb Ethernet interface speeds able to utilize the widest range of flexible connectivity options. These same networks require a variety of cost-effective cabling options for both addressing connectivity and allowing for simple migrations as network speeds and density requirements evolve. As data centers scale and bandwidth demands increase, the networking infrastructure must be capable of scaling with it. Port Breakout feature provides flexibility in splitting 100G to 4x10G, 4x25G, 2x50G cabling and vice-versa whenever requires, and hence provide Administrator a great flexibility in choosing the port speed as per their requirement. A Port Breakout group consists of 4 ports, first port will be control port and the rest 3 are subsidiary ports. Naming of Control port and its subsidiary port is as below

xe50/1, xe50/2, xe50/3, xe50/4

In xe50, numeral 50 indicates the slot of the port on a board and numerals after "/" indicates port numbers on that slot. First port (interface 50/1 in above example) is always control port whereas the rest 3 ports (ports 50/2, 50/3 and 50/4) are subsidiary ports. Only Control port can become 100G port.

Currently below breakout options are available

- 100G ports
  - 100G to 4x10G breakout ports
  - 100G to 4x25G breakout ports (due to HW limitation Autoneg isn't supported)
  - 100G to 2x50G breakout ports (due to HW limitation Autoneg isn't supported).

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.
3. One control port and subsidiary ports will be supported in 100g to 2x50G breakout
   For Example: Port XE1/1(control port) and XE1/3(subsidiary port) will be active out of 4 ports.

Terminology

Following is a brief description of terms and concepts used to describe port breakout.

Ctl: Control port

A 100G splitable port is called Control port.

Brk: Port Breakout

A control port which is split into 4x10G 4x25G or 2x50 ports.

Subsidiary ports

Ports which are members of Control Port, A subsidiary port can be Active or InActive

IA: InActive Ports

Subsidiary ports whose control port is not configured for “Port Breakout”

Removing Port Breakout

Removing Port Breakout is provided in below section.

Note: Interface xe50/1 is back to back connected and interfaces are up.

`#configure terminal`	Enter configure mode.
`(config)#interface xe50/1`	Specify the interface `(xe5/1)` to be configured for port Breakout.
`(config-if)#no port breakout`	Unconfigure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Validation

```
#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, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
--
Interface     Type             Status  Reason  Speed
Interface
--------------------------------------------------------------------------------
--
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
--
Interface    Status      Description
--------------------------------------------------------------------------------
--
lo           up          --
lo.management  up          --
```

```
-------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                      Ch #
-------------------------------------------------------------------------
--
xe1        ETH   --    routed            up      none    1g    --       Bu  No
xe2        ETH   --    routed            down    PD      10g   --       No  No
xe3        ETH   --    routed            down    PD      10g   --       No  No
xe4        ETH   --    routed            down    PD      10g   --       No  No
xe5        ETH   --    routed            down    PD      10g   --       Bu  No
xe6        ETH   --    routed            down    PD      10g   --       No  No
xe7        ETH   --    routed            down    PD      10g   --       No  No
xe8        ETH   --    routed            down    PD      10g   --       No  No
xe9        ETH   --    routed            down    PD      10g   --       Bu  No
xe10       ETH   --    routed            down    PD      10g   --       No  No
xe11       ETH   --    routed            down    PD      10g   --       No  No
xe12       ETH   --    routed            down    PD      10g   --       No  No
xe13       ETH   --    routed            down    PD      10g   --       Bu  No
xe14       ETH   --    routed            down    PD      10g   --       No  No
xe15       ETH   --    routed            down    PD      10g   --       No  No
xe16       ETH   --    routed            down    PD      10g   --       No  No
xe17       ETH   --    routed            down    PD      10g   --       Bu  No
xe18       ETH   --    routed            down    PD      10g   --       No  No
xe19       ETH   --    routed            down    PD      10g   --       No  No
xe20       ETH   --    routed            down    PD      10g   --       No  No
xe21       ETH   --    routed            down    PD      10g   --       Bu  No
xe22       ETH   --    routed            down    PD      10g   --       No  No
xe23       ETH   --    routed            down    PD      10g   --       No  No
xe24       ETH   --    routed            down    PD      10g   --       No  No
xe25       ETH   --    routed            up      none    10g   --       Bu  No
xe26       ETH   --    routed            down    PD      10g   --       No  No
xe27       ETH   --    routed            up      none    10g   --       No  No
xe28       ETH   --    routed            down    PD      10g   --       No  No
xe29       ETH   --    routed            down    PD      10g   --       Bu  No
xe30       ETH   --    routed            down    PD      10g   --       No  No
xe31       ETH   --    routed            down    PD      10g   --       No  No
xe32       ETH   --    routed            down    PD      10g   --       No  No
xe33       ETH   --    routed            down    PD      10g   --       Bu  No
xe34       ETH   --    routed            down    PD      10g   --       No  No
xe35       ETH   --    routed            down    PD      10g   --       No  No
xe36       ETH   --    routed            down    PD      10g   --       No  No
xe37       ETH   --    routed            down    PD      10g   --       Bu  No
xe38       ETH   --    routed            down    PD      10g   --       No  No
xe39       ETH   --    routed            down    PD      10g   --       No  No
xe40       ETH   --    routed            down    PD      10g   --       No  No
xe41       ETH   --    routed            down    PD      10g   --       Bu  No
xe42       ETH   --    routed            down    PD      10g   --       No  No
xe43       ETH   --    routed            down    PD      10g   --       No  No
xe44       ETH   --    routed            down    PD      10g   --       No  No
xe45       ETH   --    routed            down    PD      10g   --       Bu  No
xe46       ETH   --    routed            down    PD      10g   --       No  No
xe47       ETH   --    routed            down    PD      10g   --       No  No
xe48       ETH   --    routed            down    PD      10g   --       No  No
xe49/1     ETH   --    routed            down    PD      40g   --       Br  No
xe49/2     ETH   --    routed            down    IA      --    --       No  No
```

```
xe49/3     ETH   --    routed            down    IA      --    --       No  No
xe49/4     ETH   --    routed            down    IA      --    --       No  No
xe50/1     ETH   --    routed            up      none    40g   --       Br  No
xe50/2     ETH   --    routed            down    IA      --    --       No  No
xe50/3     ETH   --    routed            down    IA      --    --       No  No
xe50/4     ETH   --    routed            down    IA      --    --       No

#show interface xe50/1
Interface xe50/1
  Flexport: Breakout Control Port (Active): Break Out disabled
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba4  Logical:(not set)
  Port Mode is Router
  Interface index: 10053
  Metric 1 mtu 1500 duplex-full link-speed 40g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:03:20 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 20 bits/sec, 0 packets/sec
  5 minute output rate 20 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 766
    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 0 multicast packets 7 broadcast packets 0
    output packets 7 bytes 766
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/2
Interface xe50/2
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba5  Logical:(not set)
  Port Mode is Router
  Interface index: 10054
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:03:46 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
```

```
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    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 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 interface xe50/3
Interface xe50/3
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba6  Logical:(not set)
  Port Mode is Router
  Interface index: 10055
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:07:30 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    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 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 interface xe50/4
Interface xe50/4
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba7  Logical:(not set)
  Port Mode is Router
  Interface index: 10056
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
```

```
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:07:36 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    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 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
```

Here xe50/1 is a control Port whereas xe50/2, xe50/3 and xe50/4 are their subsidiary ports. The out-put shows only xe50/1 is active (interface up and running) whereas other ports are inactive (interface up but not running).

Below Outputs after applying port-breakout configured on xe50/1:

```
#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, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
--
Interface     Type             Status  Reason  Speed
Interface
--------------------------------------------------------------------------------
--
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
--
Interface    Status      Description
--------------------------------------------------------------------------------
--
lo           up          --
lo.management  up          --
```

```
-------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                      Ch #
-------------------------------------------------------------------------------
--
xe1        ETH   --    routed            up      none    1g    --       Bu  No
xe2        ETH   --    routed            down    PD      10g   --       No  No
xe3        ETH   --    routed            down    PD      10g   --       No  No
xe4        ETH   --    routed            down    PD      10g   --       No  No
xe5        ETH   --    routed            down    PD      10g   --       Bu  No
xe6        ETH   --    routed            down    PD      10g   --       No  No
xe7        ETH   --    routed            down    PD      10g   --       No  No
xe8        ETH   --    routed            down    PD      10g   --       No  No
xe9        ETH   --    routed            down    PD      10g   --       Bu  No
xe10       ETH   --    routed            down    PD      10g   --       No  No
xe11       ETH   --    routed            down    PD      10g   --       No  No
xe12       ETH   --    routed            down    PD      10g   --       No  No
xe13       ETH   --    routed            down    PD      10g   --       Bu  No
xe14       ETH   --    routed            down    PD      10g   --       No  No
xe15       ETH   --    routed            down    PD      10g   --       No  No
xe16       ETH   --    routed            down    PD      10g   --       No  No
xe17       ETH   --    routed            down    PD      10g   --       Bu  No
xe18       ETH   --    routed            down    PD      10g   --       No  No
xe19       ETH   --    routed            down    PD      10g   --       No  No
xe20       ETH   --    routed            down    PD      10g   --       No  No
xe21       ETH   --    routed            down    PD      10g   --       Bu  No
xe22       ETH   --    routed            down    PD      10g   --       No  No
xe23       ETH   --    routed            down    PD      10g   --       No  No
xe24       ETH   --    routed            down    PD      10g   --       No  No
xe25       ETH   --    routed            up      none    10g   --       Bu  No
xe26       ETH   --    routed            down    PD      10g   --       No  No
xe27       ETH   --    routed            up      none    10g   --       No  No
xe28       ETH   --    routed            down    PD      10g   --       No  No
xe29       ETH   --    routed            down    PD      10g   --       Bu  No
xe30       ETH   --    routed            down    PD      10g   --       No  No
xe31       ETH   --    routed            down    PD      10g   --       No  No
xe32       ETH   --    routed            down    PD      10g   --       No  No
xe33       ETH   --    routed            down    PD      10g   --       Bu  No
xe34       ETH   --    routed            down    PD      10g   --       No  No
xe35       ETH   --    routed            down    PD      10g   --       No  No
xe36       ETH   --    routed            down    PD      10g   --       No  No
xe37       ETH   --    routed            down    PD      10g   --       Bu  No
xe38       ETH   --    routed            down    PD      10g   --       No  No
xe39       ETH   --    routed            down    PD      10g   --       No  No
xe40       ETH   --    routed            down    PD      10g   --       No  No
xe41       ETH   --    routed            down    PD      10g   --       Bu  No
xe42       ETH   --    routed            down    PD      10g   --       No  No
xe43       ETH   --    routed            down    PD      10g   --       No  No
xe44       ETH   --    routed            down    PD      10g   --       No  No
xe45       ETH   --    routed            down    PD      10g   --       Bu  No
xe46       ETH   --    routed            down    PD      10g   --       No  No
xe47       ETH   --    routed            down    PD      10g   --       No  No
xe48       ETH   --    routed            down    PD      10g   --       No  No
```

```
xe49/1     ETH   --    routed            down    PD      40g   --       Br  No
xe49/2     ETH   --    routed            down    IA      --    --       No  No
xe49/3     ETH   --    routed            down    IA      --    --       No  No
xe49/4     ETH   --    routed            down    IA      --    --       No  No
xe50/1     ETH   --    routed            up      none    10g   --       Br Yes
xe50/2     ETH   --    routed            up      none    10g   --       No  No
xe50/3     ETH   --    routed            up      none    10g   --       No  No
xe50/4     ETH   --    routed            up      none    10g   --       No

#show interface xe50/1
Interface xe50/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba4  Logical:(not set)
  Port Mode is Router
  Interface index: 10053
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:54:58 (00:32:03 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 23 bytes 801
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 16
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 14 broadcast packets 0
    output packets 14 bytes 1532
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/2
Interface xe50/2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba5  Logical:(not set)
  Port Mode is Router
  Interface index: 10054
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:45:16 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 23 bytes 790
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 16
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 7 broadcast packets 0
    output packets 7 bytes 766
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/3
Interface xe50/3
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba6  Logical:(not set)
  Port Mode is Router
  Interface index: 10055
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:45:31 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 26 bytes 801
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 19
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 7 broadcast packets 0
    output packets 7 bytes 766
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/4
Interface xe50/4
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba7  Logical:(not set)
  Port Mode is Router
  Interface index: 10056
```

```
Metric 1 mtu 1500 duplex-full link-speed 10g
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2001 Feb 13 18:54:58 (00:33:07 ago)
Statistics last cleared: Never
inet6 fe80::aa2b:b5ff:fead:db6f/64
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
RX
  unicast packets 0 multicast packets 7 broadcast packets 0
  input packets 22 bytes 792
  jumbo packets 0
  runts 0 giants 0 CRC 0 fragments 0 jabbers 0
  input error 15
  input with dribble 0 input discard 0
  Rx pause 0
TX
  unicast packets 0 multicast packets 14 broadcast packets 0
  output packets 14 bytes 1532
  jumbo packets 0
  output errors 0 collision 0 deferred 0 late collision 0
  output discard 0
  Tx pause 0
```

Configuring Port Breakout (100G to 4x10G)

Configuring Port Breakout (100G to 4x10G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 4x10g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#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, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
```

```
-------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                       Ch #
-------------------------------------------------------------------------
--
ce1/1      ETH   --    routed            up      none    10g   --       Br Yes
ce1/2      ETH   --    routed            up      none    10g   --       No  No
ce1/3      ETH   --    routed            up      none    10g   --       No  No
ce1/4      ETH   --    routed            up      none    10g   --       No  No
```

Configuring Port Breakout (100G to 4x25G)

Configuring Port Breakout (100G to 4x25G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 4x25g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#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, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)

-------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode            Status  Reason  Speed Port    Ctl Br/Bu
Interface                                                       Ch #
-------------------------------------------------------------------------
--
ce1/1      ETH   --    routed            up      none    25g   --       Br
Yes
ce1/2      ETH   --    routed            up      none    25g   --       No  No
ce1/3      ETH   --    routed            up      none    25g   --       No  No
ce1/4      ETH   --    routed            up      none    25g   --       No  No
```

Configuring Port Breakout (100G to 2x50G)

Configuring Port Breakout (100G to 2x50G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 2x50g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#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, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                      Ch #
--------------------------------------------------------------------------------
--
ce1/1      ETH   --    routed            up      none    50g   --       Br
Yes
ce1/2      ETH   --    routed            down    IA      --    --       No  No
ce1/3      ETH   --    routed            up      none    50g   --       No  No
ce1/4      ETH   --    routed            down    IA      --    --       No  No
```

CHAPTER 17 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

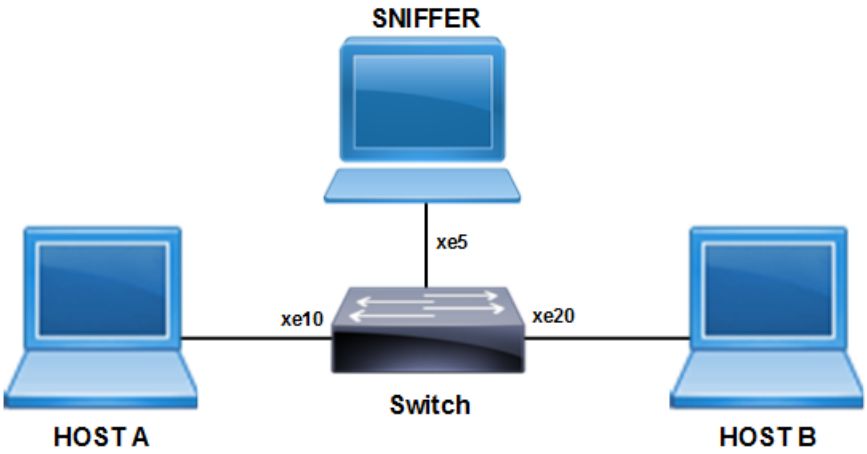


Figure 17-24: SPAN Topology

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`	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

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

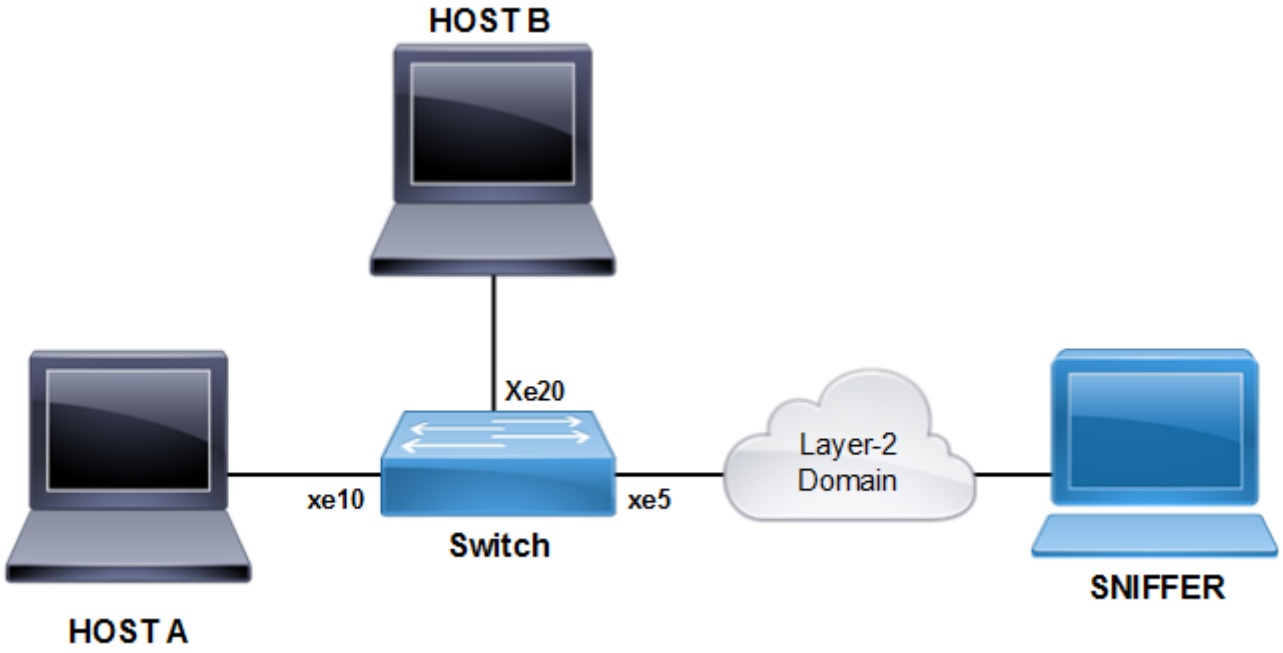


Figure 17-25: RSPAN Topology

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 18 Syslog Configuration

Syslog is a standard for logging system messages. Logging helps for fault notification, network forensics, and security auditing.

OcNOS supports logging messages to a syslog server in addition to logging to a file or on the VTY terminal (ssh/telnet connection) and on the TTY serial console device. OcNOS messages can be logged to a local syslog server (the system on which OcNOS executes) into /var/log/messages by default as well as to one or multiple remote syslog servers (maximum of 4 remote syslog server is supported). Remote syslog servers can either be configured with IPv4 addresses or host names.

Support for In-band management over default VRF

OcNOS shall stream logs to remote syslog server through the interfaces associated with management VRF by default. Also OcNOS provides configurable option to stream the logs through interfaces associated with default VRF. At any point of time OcNOS shall stream logs through only one VRF.

Topology

Figure 18-26: Syslog sample topology

Enabling rsyslog

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

Logging to a File

The below configurations 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 syslog 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 remote 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
```

Configuration to support multiple logging servers (Maximum 4 remote syslog server is supported)

`#configure terminal`	Enter Configure mode.
`(config)#hostname OcNOS`	Configuring the hostname of the device
`(config)#feature rsyslog vrf management`	Enable feature on default or management VRF. By default this feature runs on the management VRF.
`(config)#logging level all 7`	Enables debug messages for all modules.
`(config)# logging server 10.12.17.10 5 vrf management`	Redirects the log messages to the server configured. (Configuring 1 logging server).Configuring with log severity level as 5.By default severity level 7 is considered if no specific levels configured.
`(config)# logging server 10.12.17.16 5 vrf management`	Redirects the log messages to the server configured. (Configuring 2 logging server). Configuring with log severity level as 5. By default severity level 7 is considered if no specific levels configured.
`(config)# logging server 10.12.17.11 7 vrf management`	Redirects the log messages to the server configured. (Configuring 3 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
`(config)# logging server 10.12.28.22 7 vrf management`	Redirects the log messages to the server configured. (Configuring 4 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
`(config)#exit`	Exit configure mode.

Validation Commands

```
OcNOS # show running-config logging
<snippet of show running-config logging output ...>
feature rsyslog vrf management
logging server 10.12.17.10 5 vrf management
logging server 10.12.17.16 5 vrf management
logging server 10.12.17.11 7 vrf management
logging server 10.12.28.22 7 vrf management

OcNOS # show logging server
  Remote Servers:
                10.12.17.10
                severity: Operator (informational)
                facility: local7
                VRF : management
                10.12.17.16
                severity: Operator (informational)
                facility: local7
                VRF : management
                10.12.17.11
                severity: Operator (debug-detailed)
                facility: local7
```

```
VRF : management
10.12.28.22
severity: Operator (debug-detailed)
facility: local7
VRF : management
```

Remote machine Syslog Configuration:

Provided below are the changes required for rsyslog configuration on a debian system. Please refer to respective operating system official sites for more information

```
cat /etc/rsyslog.conf
$ModLoad imuxsock.so    # provides support for local system logging (e.g. via
logger command)
$ModLoad imklog.so      # provides kernel logging support (previously done by
rklogd)
$ModLoad immark.so    # provides --MARK-- message capability
$ModLoad imudp.so
$UDPServerRun 514
$ModLoad imtcp.so
$InputTCPServerRun 514
# Logs will be  placed in  separate folders based on hostnames and process
modules  in the provided path
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~

$template precise,"%msg%\n"
*.* /var/log/messages
auth,authpriv.*                 /var/log/auth.log
```

Save the changes and restart the rsyslog services to bring the changes in effect.

Monitoring Logging Server:

```
Provided below are the sample outputs collected from one of the remote logging
server.
root@localhost:~# cd /var/log/
```

Different folders I get created based on hostnames inthe defined location in rsyslog.conf

```
root@localhost:/var/log# ls -lt
drwx------ 2 root        root     4096 Nov 18 03:02 Leaf1
drwx------ 2 root        root     4096 Nov 15 07:24 10.12.56.112-leaf5
drwx------ 2 root        root     4096 Nov 15 05:40 10.12.56.109-leaf2
drwx------ 2 root        root     4096 Nov 15 01:26 Bingo1
drwx------ 2 root        root     4096 Nov 14 06:07 Leaf2
drwx------ 2 root        root     4096 Nov 11 04:57 R1-LEAF1
drwx------ 2 root        root     4096 Nov  8 06:46 leaf2
drwx------ 2 root        root     4096 Nov  8 03:38 R7-LEAF4
drwx------ 2 root        root     4096 Nov  8 01:30 LEAF1
drwx------ 2 root        root     4096 Nov  8 01:18 leaf3
drwx------ 2 root        root     4096 Nov  7 07:56 OcNOS
drwx------ 2 root        root     4096 Nov  6 23:58 mgmt-sw-3k
drwx------ 2 root        root     4096 Nov  4 21:51 R5-LEAF3
```

```
Check under OcNOS folder
root@localhost:/var/log/OcNOS# ls -ltr
```

Different log files get created based on process name under folder based on hostname.

```
-rw-r--r-- 1 root root      444 Oct 25 02:20 PSERV.log
-rw-r--r-- 1 root root      328 Oct 30 05:05 ONMD.log
-rw-r--r-- 1 root root      174 Oct 30 05:37 usermod.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 SFLOW.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 RIP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 LAG.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 VRRP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 PIM.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 OSPFv3.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 OSPF.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 IS-IS.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 802.1X.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MSTP.log
-rw-r--r-- 1 root root      483 Oct 30 07:56 HSL.log
-rw-r--r-- 1 root root      486 Oct 30 07:56 RIB.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MRIB.log
-rw-r--r-- 1 root root     8709 Nov  2 11:22 OAM.log
-rw-r--r-- 1 root root    17959 Nov  2 11:23 NSM.log
-rw-r--r-- 1 root root    12178 Nov  2 11:23 BGP.log
-rw-r--r-- 1 root root    74488 Nov  3 07:41 CMM.log
-rw-r--r-- 1 root root     4128 Nov  3 08:17 login.log
-rw-r--r-- 1 root root     5265 Nov  3 08:17 HOSTP.log
-rw-r--r-- 1 root root    21982 Nov  3 08:17 CML.log
-rw-r--r-- 1 root root 28094411 Nov  3 08:17 CMLSH.log
-rw-r--r-- 1 root root   278619 Nov  3 08:19 sshd.log
-rw-r--r-- 1 root root   695277 Nov  3 08:20 CRON.log
```

CHAPTER 19 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.
- 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

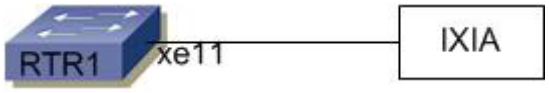


Figure 19-27: ErrDisable

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
```

Note: Stp-Bpdu-Guard is enabled by default.

```
#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
 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
---------------      ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
```

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

For transaction clients (such as NetConf), to recover a port from an error disable state manually, use this command/ RPC call:

- Command: `clear interface IFNAME error-disable`
- NetConf RPC: `interface-clear-interface-error-disable`

Note: This command/RPC applies only for an error disable state caused by an administrative shutdown. For an error disable state due to peer flapping or any other reason, recover from the error disable state by entering `shutdown` followed by `no shutdown`.

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 20 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.

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

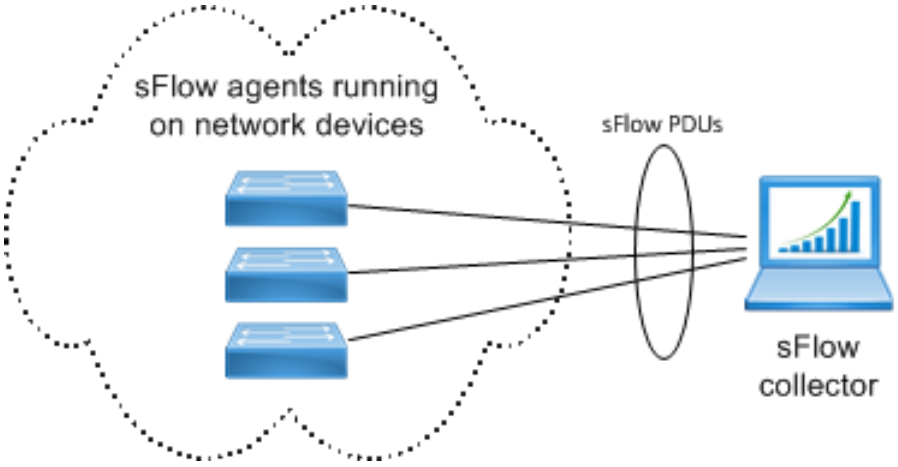


Figure 20-28: Basic sFlow topology

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 200`	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

```
OcNOS#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     200          20
```

CHAPTER 21 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 21-29: 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

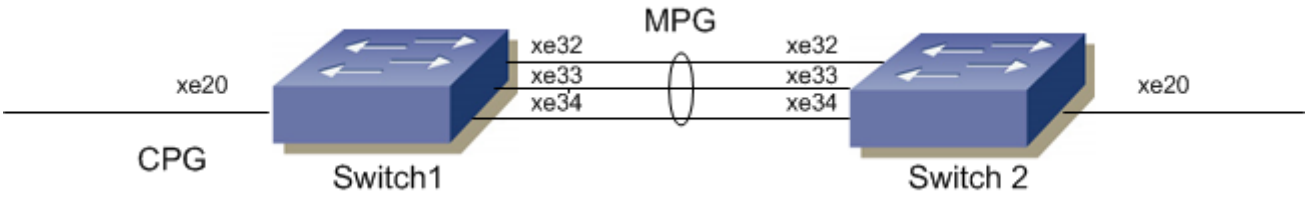


Figure 21-30: TFO with port-channel

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   --    routed           up      none    1g    --       Br  Yes
xe32      ETH   --    routed           up      none    10g   --       Br  Yes
xe33      ETH   --    routed           up      none    10g   --       No  No
xe34      ETH   --    routed           up      none    10g   --       No  No
eth0      METH                         up       --     1g
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
```

CHAPTER 22 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, and can be uploaded to a remote server. You generate a file with this information via the `show techsupport` command.

Note: Output is not displayed on the terminal.

The default directory (`/var/log/`) is where the stored information is saved. The filename has the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`. If a file name is specified, the information will be saved to `filename_YYYY_MMM_DD_HH_MM_SS_.tar.gz`. Date stamps are in the `YYYY_MM_DD` form, and time stamps are in the form `HH_MM_SS`.

The collected system data contains the following logs:

- Saved start-up configuration of the system.
- The `running-config`, and statistics for a specified module or all modules.
- The last 100 commands.
- Memory and CPU usage of the process.
- Process Id and process name.
- The user account running the process.

Tech Support Samples

`#show techsupport all`	Collects system configurations and statistics for all modules, and saves it in `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport all log-path /home/filename`	Collects system configurations and statistics for all modules, and saves it in `filename_date_timestamp.tar.gz` in the `/home/directory`.
`#show techsupport nsm`	Collects `nsm` protocol configurations and statistics, and saves it in `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport nsm log-path /home/filename`	Collects `nsm` protocol configurations and statistics, and saves it at `filename_date_timestamp.tar.gz` in the `/home/directory`.
`#show techsupport hostpd authd imi`	Collects `hostp`, `authd`, and `imi` protocol configurations and statistics and saves it at `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport hostpd authd imi log-path /home/filename`	Collects `hostp`, `authd`, `imi` protocol configurations and statistics, saves it as `filename_date_timestamp.tar.gz` in the `/home/` directory.

Validation Commands

You can display the status of a `show techsupport` command given earlier which indicates the protocol modules that have completed, are in progress, or have not executed. If the command has completed, it lists the last five generated tech support files with their path.

```
#show techsupport status

Tech Support Command Execution Is Complete
##Generated Tech Support File-list
/var/log/tech_support_18_Dec_2017_20_39_02.tar.gz
#
```

Note: the running `show techsupport` operation has not completed, reentering the `show techsupport` command is ignored.

CHAPTER 23 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 24 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 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 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 24-31 is a simple deployment using the debounce timer

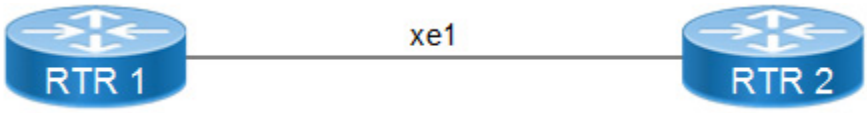


Figure 24-31: Debounce timer

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-interval 4000 ms
Flap Count: 0
Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1
Debounce timer: enabled
Debounce-interval 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-interval 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
```

CHAPTER 25 Coherent Optics Configuration

This chapter contains a coherent optics module configuration example.

Topology

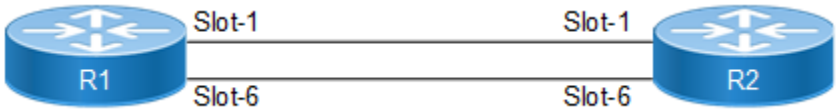


Figure 25-32: Coherent optics configuration

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 1`	Enter coherent module mode
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#modulation-format dp-qpsk`	Configure modulation format dp-qpsk
`(config-netif)#tx-laser-freq 194Thz`	Configure frequency with value 194Thz

R2

`#configure terminal`	Enter configure mode
`(config)#coherent-module 1`	Enter coherent module mode
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#modulation-format dp-qpsk`	Configure modulation format dp-qpsk
`(config-netif)#tx-laser-freq 194Thz`	Configure frequency with value 194Thz

Validation

R1

```
#show coherent-module 1
-----------------------------------------------------------------
SLOT-ID : 1
-----------------------------------------------------------------
Module Type                          :    ACO
Admin-Status                         :    UP
Oper-Status                          :    Ready
Vendor-name                          :    NEL
Vendor-SN                            :    100877111/SMV029507
Vendor-FW-Version                    :    180d.a044/101.9
```

```
Network-Interfaces                  :   1
Host-Interfaces                     :   2
CFP2 Vendor-name                    :   OCLARO
CFP2 Vendor-OUI                     :   2880
CFP2 Vendor-Part                    :   TRB100BA-02
CFP2 Vendor-SN                      :   SMV029507
CFP2 Vendor-FW-Version              :   101.9

-------------------------------------------------------------
SLOT-ID : 1   NETIF : 0
-------------------------------------------------------------
OperStatus                          :   ready
DSP-OperStatus                      :   ready
Modulation-format                   :   dp-qpsk
Differential Encoding               :   FALSE
Pulseshaping-Rx                     :   FALSE
Pulseshaping-Tx                     :   FALSE
Loopback-type                       :   none
PRBS-type                           :   none
Losi-Enabled                        :   FALSE
PRBS-IN-SYNC                        :   FALSE
Current PRBS BER                    :   nan
Current BER Period                  :   10000
Current PRE FEC BER                 :   nan
Current POST FEC BER                :   nan
Current Chromatic Dispersion        :   0
Current Differential Group Delay    :   2147483648
Tx-Disable                          :   FALSE
TX-Output-Power                     :   0.00 dBm
TX-Laser-freq                       :   194000000.000000 MHz
Min-LaserFreq                       :   191300000.000000 MHz
Max-LaserFreq                       :   196102997.874080 MHz
Current TX Laser Freq               :   194000000.000000 MHz
Grid-Spacing                        :   6.25-ghz
Laser-Grid                          :   100-ghz 50-ghz 33-ghz 25-ghz 12.5-ghz 6.25-ghz
Current Output Power                :   0.31 dBm
Current Input Power                 :   -1.55 dBm
Current Post VOA Power              :   -1.55 dBm
Current Prov~ Chnl Power            :   -34.78 dBm
Alarms                              :

-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 0
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 1
-------------------------------------------------------------
Fec-type                            :   none
```

```
Loopback-type                    :   none
```

R1

```
#show coherent-module summary
-------------------------------------------------------------------------------
Slot Status      Modulation  InputPower  LaserFreq           preFECBER    postFECBER
-------------------------------------------------------------------------------
1    Ready       dp-qpsk     -1.55 dBm   194000000.000000 MHz nan          nan
```

Coherent Optics Alarms

These alarms are generated in the multiple scenarios shown:

- RX-LOS
- RX-OTU
- [LOF] Loss-Of-Frame
- [LOM] Loss-Of-Multiframe
- RX-ODU
- [AIS] Alarm-Indication-Signal
- [OCI] Open-Connection-Indication
- RX-OPU
- [PLM] Payload-Mismatch

Table 25-2: Alarms

Alarm message	Meaning
RX-LOS (Loss of signal)	This Alarm is generated when the NE [Network Equipment] doesn't see light/signal from the far end.
OTU Alarm (OTU Alarm Indication Signal)	The local interface has received an OTU-AIS signal from the NE at the far end of the fiber, indicating that no OTN OTU signal is being transmitted upstream of (and toward) the local NE
LOF/LOM (Loss Of Frame/ Multiframe)	LOF is generated when the received frame is error or the signal is degraded [High BER]. LOM alarm occurs when the multiframe alignment process is in the out-of-multiframe (OOM) state for 3 consecutive milliseconds.
ODU (Optical Data Unit Alarm Indication Signal)	The local interface has received an ODU-AIS signal from the NE at the far end of the fiber, indicating that no OTN OTU or OTN ODU signal is being transmitted upstream of (and toward) the local NE.
BDI (Backward Defect Indication)	The local interface has received a BDI signal from the NE at the far end of the fiber, indicating that no OTN OTU signal is being transmitted downstream of (and away from) the local NE.
AIS (Alarm Indication Signal)	The local interface has received an ODU-AIS signal from the NE at the far end of the fiber, indicating that no OTN OTU or OTN ODU signal is being transmitted upstream of (and toward) the local NE.

Table 25-2: Alarms

Alarm message	Meaning
OCI (Open-Connection-Indication)	The local interface has received an ODU-OCI signal from the far-end NE, indicating that an optical cross-connect is not present on an upstream node.
OPU Alarm (Optical Channel Payload Unit)	
PLM (Payload Mismatch)	PLM is declared when the received PayloadType differs from the expected, pre-provisioned PT value

Loopback-type on Host Interface

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 1`	Enter coherent module mode
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#soft-tx-disable`	Configure soft-tx-disable
`(config-netif)#exit`	Exit network interface mode
`(config-hostif)#host-interface 0`	Enter host-interface mode
`(config-hostif)#loopback-type shallow`	Configure loopback-type as shallow
`(config-hostif)#exit`	Exit hostif mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

Validation

Initial validation before configuring soft-tx-disable.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed           up      none    100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed           up      none    100g  --       No  No
```

R2

```
R2#show interface brief | grep ce17
ce17          ETH   --    routed           up      none    100g  --       No  No
R2#show interface brief | grep ce18
ce18          ETH   --    routed           up      none    100g  --       No  No
```

After enabling soft-tx-disable on R1, verify host interfaces on both the nodes goes down.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed            down    PD      100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed            down    PD      100g  --       No  No
```

R2

```
R2#show interface brief | grep ce17
ce17          ETH   --    routed            down    PD      100g  --       No  No
R2#show interface brief | grep ce18
ce18          ETH   --    routed            down    PD      100g  --       No  No
```

After configuring host loopback on R1, verify host interface ce17 of R1 comes up.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed            up      none    100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed            down    PD      100g  --       No  No
```

Soft-tx-disable and loopback should be enabled on host interface.

```
R1#show coherent-module 1
-----------------------------------------------------------------
SLOT-ID : 1
-----------------------------------------------------------------
Module Type                          :   ACO
Admin-Status                         :   UP
Oper-Status                          :   Ready
Vendor-name                          :   NEL
Vendor-SN                            :   654659701/SMV056633
Vendor-FW-Version                    :   180d.a044/101.9
Network-Interfaces                   :   1
Host-Interfaces                      :   2
CFP2 Vendor-name                     :   OCLARO
CFP2 Vendor-OUI                      :   2880
CFP2 Vendor-Part                     :   TRB100BA-02
CFP2 Vendor-SN                       :   SMV056633
CFP2 Vendor-FW-Version               :   101.9

-----------------------------------------------------------------
SLOT-ID : 1   NETIF : 0
-----------------------------------------------------------------
OperStatus                           :   tx-off
DSP-OperStatus                       :   ready
Modulation-format                    :   dp-16-qam
Differential Encoding                :   FALSE
Pulseshaping-Rx                      :   FALSE
Pulseshaping-Tx                      :   FALSE
Loopback-type                        :   none
```

```
PRBS-type                           :   none
Losi-Enabled                        :   FALSE
PRBS-IN-SYNC                        :   FALSE
Current PRBS BER                    :   nan
Current BER Period                  :   10000
Current PRE FEC BER                 :   8.909714e-04
Current POST FEC BER                :   0.000000e+00
Current Chromatic Dispersion        :   29
Current Differential Group Delay    :   32
Tx-Disable                          :   TRUE
TX-Output-Power                     :   0.00 dBm
TX-Laser-freq                       :   193500000.000000 MHz
Min-LaserFreq                       :   191300000.000000 MHz
Max-LaserFreq                       :   196102997.874080 MHz
Current TX Laser Freq               :   193500000.000000 MHz
Grid-Spacing                        :   6.25-ghz
Laser-Grid                          :   100-ghz 50-ghz 33-ghz 25-ghz 12.5-ghz 6.
25-ghz
Current Output Power                :   -50.00 dBm
Current Input Power                 :   -2.87 dBm
Current Post VOA Power              :   -2.87 dBm
Current Prov~ Chnl Power            :   -2.68 dBm
Current OSNR Estimate               :
Alarms                              :

-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 0
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   shallow
-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 1
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
R2
R2#show interface brief | grep ce17
ce17          ETH   --    routed           down    PD      100g  --       No  No
R2#show interface brief | grep ce18
ce18          ETH   --    routed           down    PD      100g  --       No  No
```

Loopback-type on Network Interface

R1

`#configure terminal`	Enter configure mode
`(config)#interface ce17`	Enter the host interface ce17

(config)#shutdown	Perform shutdown
(config)#end	Exit interface mode
(config)#coherent-module 1	Enter coherent-module mode
(config-module)#network-interface 0	Enter networ -interface mode
(config-hostif)#loopback-type shallow	Configure loopback-type as shallow
(config-hostif)#exit	Exit hostif mode
(config-module)#exit	Exit coherent mode
(config)#exit	Exit configure mode

Validation

Initial validation before performing interface shutdown.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed            up      none    100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

R2

```
R2#show interface brief | grep ce17
ce17          ETH   --    routed            up      none    100g  --       No  No
R2#show interface brief | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

After performing shutdown on ce17 on R1, both local and remote ce17 interface should go down.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed            down    AD      100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

R2

```
R2#show interface brief | grep ce17
ce17          ETH   --    routed            down    PD      100g  --       No  No
R2#show interface brief | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

After configuring network loopback on R1, remote ce17 interface should come up.

R1

```
R1#show interface brief | grep ce17
ce17          ETH   --    routed            down    AD      100g  --       No  No
R1#show interface brief | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

Verify loopback is enabled on network interface.

```
R1#show coherent-module 1
---------------------------------------------------------------
SLOT-ID : 1
---------------------------------------------------------------
Module Type                          :   ACO
Admin-Status                         :   UP
Oper-Status                          :   Ready
Vendor-name                          :   NEL
Vendor-SN                            :   654659701/SMV056633
Vendor-FW-Version                    :   180d.a044/101.9
Network-Interfaces                   :   1
Host-Interfaces                      :   2
CFP2 Vendor-name                     :   OCLARO
CFP2 Vendor-OUI                      :   2880
CFP2 Vendor-Part                     :   TRB100BA-02
CFP2 Vendor-SN                       :   SMV056633
CFP2 Vendor-FW-Version               :   101.9

---------------------------------------------------------------
SLOT-ID : 1   NETIF : 0
---------------------------------------------------------------
OperStatus                           :   ready
DSP-OperStatus                       :   ready
Modulation-format                    :   dp-16-qam
Differential Encoding                :   FALSE
Pulseshaping-Rx                      :   FALSE
Pulseshaping-Tx                      :   FALSE
Loopback-type                        :   shallow
PRBS-type                            :   none
Losi-Enabled                         :   FALSE
PRBS-IN-SYNC                         :   FALSE
Current PRBS BER                     :   nan
Current BER Period                   :   10000
Current PRE FEC BER                  :   8.747089e-04
Current POST FEC BER                 :   0.000000e+00
Current Chromatic Dispersion         :   29
Current Differential Group Delay     :   32
Tx-Disable                           :   FALSE
TX-Output-Power                      :   0.00 dBm
TX-Laser-freq                        :   193500000.000000 MHz
Min-LaserFreq                        :   191300000.000000 MHz
Max-LaserFreq                        :   196102997.874080 MHz
Current TX Laser Freq                :   193500000.000000 MHz
Grid-Spacing                         :   6.25-ghz
Laser-Grid                           :   100-ghz 50-ghz 33-ghz 25-ghz 12.5-ghz 6.
25-ghz
Current Output Power                 :   0.47 dBm
Current Input Power                  :   -2.87 dBm
Current Post VOA Power               :   -2.87 dBm
Current Prov~ Chnl Power             :   -2.68 dBm
```

```
Current OSNR Estimate               :
Alarms                              :

-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 0
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 1
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
```

R2

```
R2#sh int br | grep ce17
ce17          ETH   --    routed            up      none    100g  --       No  No
R2#sh int br | grep ce18
ce18          ETH   --    routed            up      none    100g  --       No  No
```

Pseudo-Random Bit Stream Type

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 1`	Enter coherent-module mode
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#prbs-type prbs31`	Configure prbs-type as prbs31
`(config-hostif)#exit`	Exit hostif mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

R2

`#configure terminal`	Enter configure mode
`(config)#coherent-module 1`	Enter coherent-module mode
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#prbs-type prbs31`	Configure prbs-type as prbs31
`(config-hostif)#exit`	Exit hostif mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

Validation

Verify prbs-type is enabled and is In-Sync on both the nodes.

R1

```
R1#show coherent-module 1
------------------------------------------------------------
SLOT-ID : 1
------------------------------------------------------------
Module Type                          :   ACO
Admin-Status                         :   UP
Oper-Status                          :   Ready
Vendor-name                          :   NEL
Vendor-SN                            :   654659701/SMV056633
Vendor-FW-Version                    :   180d.a044/101.9
Network-Interfaces                   :   1
Host-Interfaces                      :   2
CFP2 Vendor-name                     :   OCLARO
CFP2 Vendor-OUI                      :   2880
CFP2 Vendor-Part                     :   TRB100BA-02
CFP2 Vendor-SN                       :   SMV056633
CFP2 Vendor-FW-Version               :   101.9
------------------------------------------------------------
SLOT-ID : 1   NETIF : 0
------------------------------------------------------------
OperStatus                           :   ready
DSP-OperStatus                       :   ready
Modulation-format                    :   dp-16-qam
Differential Encoding                :   FALSE
Pulseshaping-Rx                      :   FALSE
Pulseshaping-Tx                      :   FALSE
Loopback-type                        :   none
PRBS-type                            :   prbs31
Losi-Enabled                         :   FALSE
PRBS-IN-SYNC                         :   TRUE
Current PRBS BER                     :   0.000000e+00
Current BER Period                   :   10000
Current PRE FEC BER                  :   9.012553e-04
Current POST FEC BER                 :   0.000000e+00
Current Chromatic Dispersion         :   29
Current Differential Group Delay     :   34
Tx-Disable                           :   FALSE
TX-Output-Power                      :   0.00 dBm
TX-Laser-freq                        :   193500000.000000 MHz
Min-LaserFreq                        :   191300000.000000 MHz
Max-LaserFreq                        :   196102997.874080 MHz
Current TX Laser Freq                :   193500000.000000 MHz
Grid-Spacing                         :   6.25-ghz
Laser-Grid                           :   100-ghz 50-ghz 33-ghz 25-ghz 12.5-ghz 6.
25-ghz
```

```
Current Output Power                :   0.47 dBm
Current Input Power                 :   -2.84 dBm
Current Post VOA Power              :   -2.84 dBm
Current Prov~ Chnl Power            :   -2.63 dBm
Current OSNR Estimate               :
Alarms                              :
 RX-OPU-Alarms
                                        [CSF]Client-Signal-Fail

-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 0
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 1
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
```

R2

```
R2#show coherent-module 1
-------------------------------------------------------------
SLOT-ID : 1
-------------------------------------------------------------
Module Type                         :   ACO
Admin-Status                        :   UP
Oper-Status                         :   Ready
Vendor-name                         :   NEL
Vendor-SN                           :   100877111/SMV029507
Vendor-FW-Version                   :   180d.a044/101.9
Network-Interfaces                  :   1
Host-Interfaces                     :   2
CFP2 Vendor-name                    :   OCLARO
CFP2 Vendor-OUI                     :   2880
CFP2 Vendor-Part                    :   TRB100BA-02
CFP2 Vendor-SN                      :   SMV029507
CFP2 Vendor-FW-Version              :   101.9

-------------------------------------------------------------
SLOT-ID : 1   NETIF : 0
-------------------------------------------------------------
OperStatus                          :   ready
DSP-OperStatus                      :   ready
Modulation-format                   :   dp-16-qam
Differential Encoding               :   FALSE
Pulseshaping-Rx                     :   FALSE
Pulseshaping-Tx                     :   FALSE
Loopback-type                       :   none
PRBS-type                           :   prbs31
```

```
Losi-Enabled                          :   FALSE
PRBS-IN-SYNC                          :   TRUE
Current PRBS BER                      :   0.000000e+00
Current BER Period                    :   10000
Current PRE FEC BER                   :   4.886308e-03
Current POST FEC BER                  :   0.000000e+00
Current Chromatic Dispersion          :   21
Current Differential Group Delay      :   71
Tx-Disable                            :   FALSE
TX-Output-Power                       :   0.00 dBm
TX-Laser-freq                         :   193500000.000000 MHz
Min-LaserFreq                         :   191300000.000000 MHz
Max-LaserFreq                         :   196102997.874080 MHz
Current TX Laser Freq                 :   193500000.000000 MHz
Grid-Spacing                          :   6.25-ghz
Laser-Grid                            :   100-ghz 50-ghz 33-ghz 25-ghz 12.5-ghz 6.
25-ghz
Current Output Power                  :   0.13 dBm
Current Input Power                   :   -1.57 dBm
Current Post VOA Power                :   -1.57 dBm
Current Prov~ Chnl Power              :   -1.43 dBm
Current OSNR Estimate                 :
Alarms                                :
 RX-OPU-Alarms
                                          [CSF]Client-Signal-Fail

-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 0
-------------------------------------------------------------
Fec-type                              :   none
Loopback-type                         :   none
-------------------------------------------------------------
SLOT-ID : 1   HOSTIF : 1
-------------------------------------------------------------
Fec-type                              :   none
Loopback-type                         :   none
```

Rx-Power User-Defined Threshold Alarms

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#network-interface 0`	Enter network interface mode

(config-netif)#threshold rx-power high-alarm -5 high-warning -10 low-warning -15 low-alarm -20	Configure rx-power threshold values
(config-netif)#exit	Exit network interface mode
(config-module)#exit	Exit coherent mode
(config)#exit	Exit configure mode

R2

#configure terminal	Enter configure mode
(config)#coherent-module 6	Enter coherent-module mode
(config-module)#enable	Enable coherent-module
(config-module)#exit	Exit coherent mode
(config)#exit	Exit configure mode

Validation

R1

```
R1#show running-config coherent-module
!
coherent-module 1
 enable
!
coherent-module 6
 enable
 !
  network-interface 0
  threshold rx-power high-alarm -5.00 high-warning -10.00 low-warning -15.00 low-alarm -
20.00
  exit
!

R1#show coherent-module 6 monitoring-thresholds
---------------------------------------------------------------
Temperature [44.62 °C] : Moniotoring Enabled
---------------------------------------------------------------
Temperature HIGH Alarm threshold    : 80.00 °C
Temperature HIGH Warning threshold  : 75.00 °C
Temperature LOW Warning threshold   : 0.00 °C
Temperature LOW Alarm threshold     : -5.00 °C

---------------------------------------------------------------
Voltage [3.336 V] : Moniotoring Enabled
---------------------------------------------------------------
Voltage HIGH Alarm threshold        : 3.000 V
Voltage HIGH Warning threshold      : 3.100 V
Voltage LOW Warning threshold       : 3.600 V
```

```
Voltage LOW Alarm threshold         : 3.500 V

------------------------------------------------------------
Input-Power [-0.13 dBm] : Moniotoring Enabled
------------------------------------------------------------
Input-Power HIGH Alarm threshold    : -5.00 dBm
Input-Power HIGH Warning threshold  : -10.00 dBm
Input-Power LOW Warning threshold   : -15.00 dBm
Input-Power LOW Alarm threshold     : -20.00 dBm
Permissible Input-Power HIGH Alarm threshold range   : -11.00 dBm to 8.00 dBm
Permissible Input-Power HIGH Warning threshold range : -11.10 dBm to 6.99 dBm
Permissible Input-Power LOW Warning threshold range  : -30.00 dBm to 5.99 dBm
Permissible Input-Power LOW Alarm threshold range    : -40.00 dBm to 5.00 dBm

------------------------------------------------------------
Output-Power [-0.01 dBm] : Moniotoring Enabled
------------------------------------------------------------
Output-Power HIGH Alarm threshold   : 5.00 dBm
Output-Power HIGH Warning threshold : 3.50 dBm
Output-Power LOW Warning threshold  : -11.00 dBm
Output-Power LOW Alarm threshold    : -12.00 dBm

------------------------------------------------------------
Pre-FEC BER [5.898595e-04] : Moniotoring Disabled
------------------------------------------------------------
Prefec signal-failure threshold     : 0.000000e+00
Prefec signal-degrade threshold     : 0.000000e+00
Prefec signal-clear threshold       : 0.000000e+00
```

Rx-Power High-Alarm Threshold

Note: When rx-power reaches high-alarm threshold, the below operator logs will be generated on the terminal.

```
R1#2000 Jan 01 05:40:16.917 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif Input-Power High-
Alarm Detected for Slot: 6 , Netif: 0


R1#show coherent-module 6 faws
------------------------------------------------------------
                         Fault & Status
------------------------------------------------------------

------------------------------------------------------------
                         Alarm and Warning
------------------------------------------------------------

Network-Lane 0 Alarm & Warning      :
   Input-Power                      : Input-Power High-Alarm

R1#show coherent-module 6
```

```
---------------------------------------------------------------
SLOT-ID : 6
---------------------------------------------------------------
Module Type                          :   DCO
Admin-Status                         :   UP
Oper-Status                          :   Ready
Vendor-name                          :   LUMENTUM
Vendor-SN                            :   VCD19330008
Vendor-FW-Version                    :   1.5
Network-Interfaces                   :   1
Host-Interfaces                      :   2
CFP2 Vendor-name                     :   LUMENTUM
CFP2 Vendor-OUI                      :   0xF00200
CFP2 Vendor-Part                     :   TRB200DAA-01
CFP2 Vendor-SN                       :   VCD19330008
CFP2 Vendor-FW-Version               :   1.5
CFP2 Temperature                     :   44.56 °C
CFP2 Power Supply                    :   3.336 V

---------------------------------------------------------------
SLOT-ID : 6   NETIF : 0
---------------------------------------------------------------
OperStatus                           :   ready
DSP-OperStatus                       :   ready
Modulation-format                    :   dp-16-qam
Differential Encoding                :   FALSE
Pulseshaping-Rx                      :
Pulseshaping-Tx                      :   FALSE
Loopback-type                        :   none
PRBS-type                            :   none
Losi-Enabled                         :
PRBS-IN-SYNC                         :   FALSE
Current PRBS BER                     :   nan
Current BER Period                   :   1000 ms
Current PRE FEC BER                  :   5.840260e-04
Current POST FEC BER                 :
Current Chromatic Dispersion         :   0 ps/nm
Current Differential Group Delay     :   6 ps
Tx-Disable                           :   FALSE
TX-Output-Power                      :   0.00 dBm
TX-Laser-freq                        :   193500000.000000 MHz
Min-LaserFreq                        :   191150000.000000 MHz
Max-LaserFreq                        :   196100000.000000 MHz
Current TX Laser Freq                :   193500000.000000 MHz
Grid-Spacing                         :   6.25-ghz
Laser-Grid                           :   100-ghz 50-ghz 25-ghz 12.5-ghz 6.25-ghz
Current Output Power                 :   -0.01 dBm
Current Input Power                  :   -0.13 dBm
Current Post VOA Power               :
Current Prov~ Chnl Power             :   -1.16 dBm
```

```
Current Post VOA Prov~ Chnl Power   :   -1.16 dBm
Current OSNR Estimate               :   33.70 dB
Current Q-Margin                    :   3.30 dB
Current Uncorrected Block-count     :   0

-------------------------------------------------------------
SLOT-ID : 6   HOSTIF : 0
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none

-------------------------------------------------------------
SLOT-ID : 6   HOSTIF : 1
-------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none

R1#show coherent-module summary
-----------------------------------------------
Slot License Information
-----------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------
------------------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
 LaserFreq

-------------------------------------------------------------------------------
------------------
1    Ready                ready            dp-16-qam   -0.03dBm    2.297608e-03
 193.500000THz
6    Ready         SET    ready            dp-16-qam   -0.13dBm    5.396472e-04
 193.500000THz
```

Rx-power High-Warning Threshold

Note: Whenever rx-power reaches high-warning threshold, the below operator logs will be generated on the terminal.

```
R1#2000 Jan 01 05:43:15.917 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif Input-Power High-
Warning Detected for Slot: 6 , Netif: 0

R1#show coherent-module 6 | grep Input
Current Input Power                 :   -8.14 dBm

R1#show coherent-module 6 faws
-------------------------------------------------------------
                        Fault & Status
```

```
------------------------------------------------------------

------------------------------------------------------------
                        Alarm and Warning
------------------------------------------------------------

Network-Lane 0 Alarm & Warning      :
   Input-Power                      : Input-Power High-Warning

R1#show coherent-module summary
---------------------------------------------
Slot License Information
---------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------
------------------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
 LaserFreq
-------------------------------------------------------------------------------
------------------
1    Ready                ready            dp-16-qam   -0.03dBm    2.287763e-03
 193.500000THz
6    Ready         SET    ready            dp-16-qam   -8.14dBm    5.867256e-04
 193.500000THz
```

Rx-power Low-Warning Threshold

Note: When rx-power reaches Low-warning threshold the below operator logs will be generated on the terminal

```
R1#2000 Jan 01 05:44:27.935 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif Input-Power Low-
Warning Detected for Slot: 6 , Netif: 0

R1#show coherent-module 6 | grep Input
Current Input Power                 :   -15.17 dBm

R1#show coherent-module 6 faws
------------------------------------------------------------
                        Fault & Status
------------------------------------------------------------

------------------------------------------------------------
                        Alarm and Warning
------------------------------------------------------------

Network-Lane 0 Alarm & Warning      :
   Input-Power                      : Input-Power Low-Warning
```

```
R1#show coherent-module summary
---------------------------------------------
Slot License Information
---------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------
------------------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
 LaserFreq

-------------------------------------------------------------------------------
------------------
1    Ready                ready           dp-16-qam   -0.03dBm    2.257144e-03
 193.500000THz
6    Ready         SET    ready           dp-16-qam   -15.17dBm   7.625295e-04
 193.500000THz
```

Rx-power Low-Alarm Threshold

Note: Whenever rx-power reaches low-Alarm threshold, the below operator logs will be generated on the terminal.

```
R1#2000 Jan 01 05:45:00.917 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Current Module General
Status for Slot: 6 not OK
Module General Status : RX-Loss-Of-Signal
2000 Jan 01 05:45:00.917 : OcNOS : CMM : CRITI : [CMM_TAI_2]: RX-LOS alarm Detected for
Slot: 6 Netif: 0
2000 Jan 01 05:45:00.917 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif Input-Power Low-
Alarm Detected for Slot: 6 , Netif: 0

R1#show coherent-module 6 | grep Input
Current Input Power                 :   -20.23 dBm

R1#show coherent-module 6 faws
---------------------------------------------------------------
                         Fault & Status
---------------------------------------------------------------
Module General Status               : RX-Loss-Of-Signal
Network-Lane 0 Fault & Status       : RX-LOS-Alarm

---------------------------------------------------------------
                         Alarm and Warning
---------------------------------------------------------------

Network-Lane 0 Alarm & Warning      :
   Input-Power                      : Input-Power Low-Alarm

R1#show coherent-module summary
---------------------------------------------
```

```
Slot License Information
------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------
------------------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
 LaserFreq

-------------------------------------------------------------------------------
------------------
1    Ready                ready            dp-16-qam   -0.03dBm    2.275678e-03
 193.500000THz
6    Initialize    SET    ready            dp-16-qam   -20.23dBm   1.463204e-03
 193.500000THz
```

Pre-FEC BER User-Defined Threshold Alarms

Pre-FEC BER Signal-Failure Threshold

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#threshold pre-fec-ber signal-failure 5e-04 signal-degrade 5e-05 clear 5e-06`	Configure Pre-FEC BER threshold values
`(config-netif)#exit`	Exit network interface mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

R2

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

Validation

R1:

```
R1#show running-config coherent-module
!
coherent-module 1
 enable
!
coherent-module 6
 enable
 !
  network-interface 0
  threshold pre-fec-ber signal-failure 5.00e-04 signal-degrade 5.00e-05 clear 5.00e-06
  exit
!

R1#show coherent-module 6 monitoring-thresholds
---------------------------------------------------------------
Temperature [44.81 °C] : Moniotoring Enabled
---------------------------------------------------------------
Temperature HIGH Alarm threshold    : 80.00 °C
Temperature HIGH Warning threshold  : 75.00 °C
Temperature LOW Warning threshold   : 0.00 °C
Temperature LOW Alarm threshold     : -5.00 °C

---------------------------------------------------------------
Voltage [3.336 V] : Moniotoring Enabled
---------------------------------------------------------------
Voltage HIGH Alarm threshold        : 3.000 V
Voltage HIGH Warning threshold      : 3.100 V
Voltage LOW Warning threshold       : 3.600 V
Voltage LOW Alarm threshold         : 3.500 V

---------------------------------------------------------------
Input-Power [-0.13 dBm] : Moniotoring Enabled
---------------------------------------------------------------
Input-Power HIGH Alarm threshold    : 4.00 dBm
Input-Power HIGH Warning threshold  : 3.00 dBm
Input-Power LOW Warning threshold   : -24.09 dBm
Input-Power LOW Alarm threshold     : -25.09 dBm
Permissible Input-Power HIGH Alarm threshold range   : -11.00 dBm to 8.00 dBm
Permissible Input-Power HIGH Warning threshold range : -11.10 dBm to 6.99 dBm
Permissible Input-Power LOW Warning threshold range  : -30.00 dBm to 5.99 dBm
Permissible Input-Power LOW Alarm threshold range    : -40.00 dBm to 5.00 dBm

---------------------------------------------------------------
Output-Power [-0.11 dBm] : Moniotoring Enabled
---------------------------------------------------------------
Output-Power HIGH Alarm threshold   : 5.00 dBm
Output-Power HIGH Warning threshold : 3.50 dBm
```

```
Output-Power LOW Warning threshold  : -11.00 dBm
Output-Power LOW Alarm threshold    : -12.00 dBm

------------------------------------------------------------
Pre-FEC BER [5.674798e-04] : Moniotoring Enabled (User-Thresholds)
------------------------------------------------------------
Prefec signal-failure threshold     : 5.000000e-04
Prefec signal-degrade threshold     : 5.000000e-05
Prefec signal-clear threshold       : 5.000000e-06
```

Note: When pre-fec reaches signal-failure threshold, the below operator logs will be generated on the terminal.

```
R1#2000 Jan 02 05:13:17.905 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif PreFECBER Sig-nal
Failure Alarm Detected for Slot: 6 , Netif: 0


R1#show coherent-module 6 faws
------------------------------------------------------------
                        Fault & Status
------------------------------------------------------------

------------------------------------------------------------
                        Alarm and Warning
------------------------------------------------------------

Network-Lane 0 Alarm & Warning      :
   preFECBER Signal                 : PreFECBER Signal Failure Alarm

R1#show coherent-module 6 | grep PRE
Current PRE FEC BER                 :   5.580834e-04

R1#show coherent-module summary
-----------------------------------------------
Slot License Information
-----------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------------------
-----------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
LaserFreq

-------------------------------------------------------------------------------------------
-----------
1    Ready               ready           dp-16-qam   -0.03dBm    2.242277e-03
193.500000THz
6    Ready         SET   ready           dp-16-qam   -0.12dBm    5.946857e-04
193.500000THz
```

Pre-FEC BER Signal-Degrade Threshold

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#threshold pre-fec-ber signal-failure 5.00e-03 signal-degrade 5.00e-04 clear 5.00e-05`	Configure Pre-FEC BER threshold values
`(config-netif)#exit`	Exit network interface mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

R2

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

Validation

R1:

```
R1#show running-config coherent-module
!
coherent-module 1
 enable
!
coherent-module 6
 enable
 !
  network-interface 0
  threshold pre-fec-ber signal-failure 5.00e-03 signal-degrade 5.00e-04 clear 5.00e-05
  exit
!

R1#show coherent-module 6 monitoring-thresholds
-----------------------------------------------------------------
Temperature [44.41 °C] : Moniotoring Enabled
-----------------------------------------------------------------
Temperature HIGH Alarm threshold    : 80.00 °C
Temperature HIGH Warning threshold  : 75.00 °C
Temperature LOW Warning threshold   : 0.00 °C
```

```
Temperature LOW Alarm threshold     : -5.00 °C

------------------------------------------------------------
Voltage [3.336 V] : Moniotoring Enabled
------------------------------------------------------------
Voltage HIGH Alarm threshold        : 3.000 V
Voltage HIGH Warning threshold      : 3.100 V
Voltage LOW Warning threshold       : 3.600 V
Voltage LOW Alarm threshold         : 3.500 V

------------------------------------------------------------
Input-Power [-0.13 dBm] : Moniotoring Enabled
------------------------------------------------------------
Input-Power HIGH Alarm threshold    : 4.00 dBm
Input-Power HIGH Warning threshold  : 3.00 dBm
Input-Power LOW Warning threshold   : -24.09 dBm
Input-Power LOW Alarm threshold     : -25.09 dBm
Permissible Input-Power HIGH Alarm threshold range   : -11.00 dBm to 8.00 dBm
Permissible Input-Power HIGH Warning threshold range : -11.10 dBm to 6.99 dBm
Permissible Input-Power LOW Warning threshold range  : -30.00 dBm to 5.99 dBm
Permissible Input-Power LOW Alarm threshold range    : -40.00 dBm to 5.00 dBm

------------------------------------------------------------
Output-Power [-0.11 dBm] : Moniotoring Enabled
------------------------------------------------------------
Output-Power HIGH Alarm threshold   : 5.00 dBm
Output-Power HIGH Warning threshold : 3.50 dBm
Output-Power LOW Warning threshold  : -11.00 dBm
Output-Power LOW Alarm threshold    : -12.00 dBm

------------------------------------------------------------
Pre-FEC BER [5.627871e-04] : Moniotoring Enabled (User-Thresholds)
------------------------------------------------------------
Prefec signal-failure threshold     : 5.000000e-03
Prefec signal-degrade threshold     : 5.000000e-04
Prefec signal-clear threshold       : 5.000000e-05
```

Note: When pre-fec reaches signal-degrade threshold the below operator logs will be generated on the terminal.

```
R1#2000 Jan 02 05:24:24.905 : OcNOS : CMM : CRITI : [CMM_TAI_2]: Netif PreFECBER Sig-nal
Degrade Alarm Detected for Slot: 6 , Netif: 0


R1#show coherent-module 6 faws
------------------------------------------------------------
                         Fault & Status
------------------------------------------------------------

------------------------------------------------------------
                         Alarm and Warning
------------------------------------------------------------
```

```
Network-Lane 0 Alarm & Warning      :
   preFECBER Signal                 : PreFECBER Signal Degrade Alarm

R1#show coherent-module 6 | grep PRE
Current PRE FEC BER                 :   5.716924e-04

R1#show coherent-module summary
---------------------------------------------
Slot License Information
---------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------------------
-----------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
LaserFreq

-------------------------------------------------------------------------------------------
-----------
1    Ready                ready            dp-16-qam   -0.03dBm    2.280438e-03
193.500000THz
6    Ready         SET    ready            dp-16-qam   -0.13dBm    5.711457e-04
193.500000THz
```

Pre-FEC BER Signal-Clear Threshold

R1

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module
`(config-module)#network-interface 0`	Enter network interface mode
`(config-netif)#threshold pre-fec-ber signal-failure 5.00e-02 signal-degrade 5.00e-03 clear 5.00e-04`	Configure Pre-FEC BER threshold values
`(config-netif)#exit`	Exit network interface mode
`(config-module)#exit`	Exit coherent mode
`(config)#exit`	Exit configure mode

R2

`#configure terminal`	Enter configure mode
`(config)#coherent-module 6`	Enter coherent-module mode
`(config-module)#enable`	Enable coherent-module

(config-module)#exit	Exit coherent mode
(config)#exit	Exit configure mode

Validation

```
R1
R1#show running-config coherent-module
!
coherent-module 1
 enable
!
coherent-module 6
 enable
 !
  network-interface 0
  threshold pre-fec-ber signal-failure 5.00e-02 signal-degrade 5.00e-03 clear 5.00e-04
  exit
!

R1#show coherent-module 6 monitoring-thresholds
-----------------------------------------------------------------
Temperature [44.61 °C] : Moniotoring Enabled
-----------------------------------------------------------------
Temperature HIGH Alarm threshold    : 80.00 °C
Temperature HIGH Warning threshold  : 75.00 °C
Temperature LOW Warning threshold   : 0.00 °C
Temperature LOW Alarm threshold     : -5.00 °C

-----------------------------------------------------------------
Voltage [3.336 V] : Moniotoring Enabled
-----------------------------------------------------------------
Voltage HIGH Alarm threshold        : 3.000 V
Voltage HIGH Warning threshold      : 3.100 V
Voltage LOW Warning threshold       : 3.600 V
Voltage LOW Alarm threshold         : 3.500 V

-----------------------------------------------------------------
Input-Power [-0.12 dBm] : Moniotoring Enabled
-----------------------------------------------------------------
Input-Power HIGH Alarm threshold    : 4.00 dBm
Input-Power HIGH Warning threshold  : 3.00 dBm
Input-Power LOW Warning threshold   : -24.09 dBm
Input-Power LOW Alarm threshold     : -25.09 dBm
Permissible Input-Power HIGH Alarm threshold range   : -11.00 dBm to 8.00 dBm
Permissible Input-Power HIGH Warning threshold range : -11.10 dBm to 6.99 dBm
Permissible Input-Power LOW Warning threshold range  : -30.00 dBm to 5.99 dBm
Permissible Input-Power LOW Alarm threshold range    : -40.00 dBm to 5.00 dBm

-----------------------------------------------------------------
Output-Power [-0.11 dBm] : Moniotoring Enabled
```

```
-------------------------------------------------------------
Output-Power HIGH Alarm threshold   : 5.00 dBm
Output-Power HIGH Warning threshold : 3.50 dBm
Output-Power LOW Warning threshold  : -11.00 dBm
Output-Power LOW Alarm threshold    : -12.00 dBm

-------------------------------------------------------------
Pre-FEC BER [5.615749e-04] : Moniotoring Enabled (User-Thresholds)
-------------------------------------------------------------
Prefec signal-failure threshold     : 5.000000e-02
Prefec signal-degrade threshold     : 5.000000e-03
Prefec signal-clear threshold       : 5.000000e-04
```

Note: When pre-fec reaches signal-clear threshold the below operator logs will be generated on the terminal.

```
R1#2020 Jul 28 10:33:57.155 : OcNOS : CMM : NOTIF : [CMM_TAI_4]: Netif PreFECBER Alarm/
Warning Cleared for Slot: 6

R1#show coherent-module 6 faws
-------------------------------------------------------------
                         Fault & Status
-------------------------------------------------------------

-------------------------------------------------------------
                         Alarm and Warning
-------------------------------------------------------------

R1#show coherent-module 6 | grep PRE
Current PRE FEC BER                 :   5.503155e-04

R1#show coherent-module summary
-----------------------------------------------
Slot License Information
-----------------------------------------------
Maximum Licenses     : 2
Available Licenses   : 0
Used Licenses        : 2 [Slots : 1, 6]

-------------------------------------------------------------------------------------------
-----------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
LaserFreq

-------------------------------------------------------------------------------------------
-----------
1    Ready                ready            dp-16-qam   -0.03dBm    2.279180e-03
193.500000THz
6    Ready         CLEAR  ready            dp-16-qam   -0.12dBm    5.509956e-04
193.500000THz
```

System Management Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Basic Commands

This chapter describes basic commands.

- show nsm client
- show privilege
- show process
- show running-config
- show startup-config
- show timezone
- show users
- show version
- sys-reload
- sys-shutdown
- terminal length
- terminal monitor
- traceroute
- write
- write terminal

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 write 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
```

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

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#clock timezone Los_Angeles
```

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
(config)#
```

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 write 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]
#
```

debug nsm

Use this command to enable NSM debugging.

Use the `no` form of this command or the `undebug` command to disable NSM debugging.

Command Syntax

```
debug nsm (all|)
no debug nsm (all|)
undebug nsm (all|)

debug nsm bfd
no debug nsm bfd
undebug nsm bfd

debug nsm events
no debug nsm events
undebug nsm events

debug nsm hal (all|) debug
debug nsm hal events
no debug nsm hal (all|)
no debug nsm hal events
undebug nsm hal events

debug nsm packet (recv|send|) (detail|)
no debug nsm packet (recv|send|) (detail|)
undebug nsm packet (recv|send|) (detail|)
```

Parameters

`all`	Enable all debugging.
`bfd`	Debug BFD events.
`events`	Debug NSM events.
`hal`	Debug HAL.
`events`	Debug HAL events.
`packet`	Debug packet events.
`recv`	Debug received packets.
`send`	Debug sent packets.
`detail`	Show detailed packet information.

Default

By default, debugging is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug nsm all
#
#debug nsm bfd
#
#debug nsm events
#
#debug nsm hal all
#
#debug nsm packet
#
#debug nsm packet recv detail
```

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
>
```

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`.

Note: The `do` command supports only the following CLI commands only

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
#
```

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.

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 clear text password. First, use this command to create a plain password. Then, use the service password-encryption command to encrypt the password. An encrypted password display as an encrypted string in configuration file.

Hidden Password

A hidden password is same as an encrypted which is already encrypted. You do not need the service password-encryption command for this method.

Note: Use the above Hidden password method only if you know the encrypted string of the plain text string that you want to use as a password.

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`	The HIDDEN “enable” password string.

Note: Password can be an alpha-numeric string between 6-32 characters, including spaces. the string cannot begin with a number.

Default

None

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 write 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 lin”e VTY mode.

Command Syntax

```
line vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.8.

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.

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.

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 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.

```
>logout
OcNOS login:

>enable
en#logout
>
```

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
```

ping (interactive)

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 1-3:

Table 1-3: 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
```

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]#
```

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

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.

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

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 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 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 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 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 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 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
#
```

show process

Use this command to display the OcNOS daemon processes that are running.

Command Syntax

```
show process
```

Parameters

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          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 1-4 explains the output fields.

Table 1-4: 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

```
(config)#show running-config
no service password-encryption
!
no service dhcp
ip domain-lookup
!
mpls propagate-ttl
!
vrrp vmac enable
spanning-tree mode provider-rstp
!
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 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 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|chile|europe|indian|mexico|pacific|us)
```

Parameters

`africa`	Africa timezone list
`all`	All timezone list
`america`	America timezone list
`antarctica`	Antarctica timezone list
`arctic`	Arctic 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

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS 1.3.7

Examples

```
#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
```

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
```

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 1-5: 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 1-5: 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

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

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.

Command Syntax

```
sys-shutdown
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

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?
```

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.

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

By default, terminal length is 25 lines.

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 Privileged Virtual Router (PVR) or VR user. When the command is used without a parameter, it can be used by a PVR user or non-PVR user to display the debug output on the terminal for the user local VR. When used with a parameter, it may be used only by a PVR user.

The `no` form of the command terminates the debug output on the terminal. Both the PVR and VR user can use this command. In addition, the PVR 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
```

traceroute

Use this command to trace an IPv4/v6 route to its destination.

Command Syntax

```
traceroute WORD
traceroute 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

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]
```

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 2 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
```

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 2-6

Table 2-6: 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

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 3 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 4 DHCP Snooping Commands

This chapter provides a description of the syntax and examples DHCP snooping. It includes the following commands:

clear ip dhcp snooping binding

Use this command to remove all entries from the binding table.

Command Syntax

```
clear ip dhcp snooping (source|) binding bridge <1-32>
```

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip dhcp snooping binding bridge 1
```

debug ip dhcp snooping

Use this command to enable the debugging DHCP snooping.

Use the `no` parameter to disable the debug options.

Command Syntax

```
debug ip dhcp snooping (event|rx|tx|packet|all)
no debug ip dhcp snooping (event|rx|tx|packet|all)
```

Parameters

`event`	Enable event debugging
`rx`	Enable receive debugging
`tx`	Enable transmit debugging
`packet`	Enable packet debugging
`all`	Enable all debugging

Default

By default all debugging options are disabled.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip dhcp snooping all
#no debug ip dhcp snooping packet
```

ip dhcp packet strict-validation

Use this command to enable strict validation of DHCP packets. Strict validation of the DHCP packet checks that the DHCP option field in the packet is valid including the magic cookie value in the first four bytes of the options field. The device drops the packet if validation fails.

Use the `no` parameter to disable strict validation.

Command Syntax

```
ip dhcp packet strict-validation bridge <1-32>
no ip dhcp packet strict-validation bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default strict validation of the DHCP packets is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config termminal
(config)#ip dhcp packet strict-validation bridge 1
(config)#no ip dhcp packet strict-validation bridge 1
```

ip dhcp snooping

Use this command to enable DHCP snooping on the bridge level.

Use the `no` parameter to remove the entire DHCP snooping configuration.

Command Syntax

```
ip dhcp snooping bridge <1-32>
no ip dhcp snooping bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default dhcp snooping will be disabled on the bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping bridge 1
(config)#no ip dhcp snooping bridge 1
```

ip dhcp snooping binding

Use this command to create a static binding entry in the binding table. All the DHCP responses will be validated against the static entries. If the response does not match the entry in the binding table, the response packet is dropped.

Use the `no` parameter to remove an entry from the binding table.

Command Syntax

```
ip dhcp snooping binding bridge <1-32> XXXX.XXXX.XXXX <1-4094> (ipv4 A.B.C.D | ipv6
  X:X::X:X) IFNAME
no ip dhcp snooping binding bridge <1-32> XXXX.XXXX.XXXX <1-4094> (ipv4 | ipv6 )
```

Parameters

`<1-32>`	Bridge number
`XXXX.XXXX.XXXX`	MAC address
`<1-4094>`	VLAN identifier
`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`IFNAME`	Interface name

Default

By default binding table will not have any entry

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping binding bridge 1 0001.0002.0003 2 ipv4 12.0.0.1 xe1
(config)#no ip dhcp snooping binding bridge 1 0001.0002.0003 2 ipv4
```

ip dhcp snooping database

Use this command to write the entries in the binding table to persistent storage.

Command Syntax

```
ip dhcp snooping database bridge <1-32>
```

Parameters

<1-32>	Bridge number

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#ip dhcp snooping database bridge 1
```

ip dhcp snooping information option

Use this command to insert option 82 information into DHCP packets.

Use the `no` parameter to disable inserting option 82.

Command Syntax

```
ip dhcp snooping information option bridge <1-32>
no ip dhcp snooping information option bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default address option 82 information insertion is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping information option bridge 1
(config)#no ip dhcp snooping information option bridge 1
```

ip dhcp snooping ratelimit

Use this command to limit the rate of DHCP packets per second.

Use the no parameter to set the rate limit to its default value (100 pps).

Command Syntax

```
ip dhcp snooping ratelimit RATELIMIT bridge <1-32>
no ip dhcp snooping ratelimit bridge <1-32>
```

Parameters

RATELIMIT	Packets per second <0-2048>
<1-32>	Bridge number

Default

The default rate limit value is 100 packets per second.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping ratelimit 2000 bridge 1
(config)#no ip dhcp snooping ratelimit bridge 1
```

ip dhcp snooping trust

Use this command to mark an interface as trusted. All DHCP servers must be connected to the trusted interface.

Use the `no` parameter to remove an interface from the list of trusted interfaces.

Command Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Parameters

None

Default

By default all interfaces are untrusted.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ip dhcp snooping trust
(config-if)#no ip dhcp snooping trust
```

ip dhcp snooping verify mac-address

Use this command to enable the DHCP snooping MAC address verification. If the device receives a DHCP request packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, the device drops the packet.

Use the `no` parameter to disable the address verification.

Command Syntax

```
ip dhcp snooping verify mac-address bridge <1-32>
no ip dhcp snooping verify mac-address bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default address verification is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping verify mac-address bridge 1
(config)#no ip dhcp snooping verify mac-address bridge 1
```

ip dhcp snooping vlan

Use this command to enable DHCP snooping for the given VLAN.

Use the `no` parameter to disable the DHCP snooping on the VLAN.

Command Syntax

```
ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32>
no ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32>
```

Parameters

`VLAN_RANGE2`	VLAN identifier <1-4094>
`<1-32>`	Bridge number

Default

By default DHCP snooping will be disabled on all the vlans

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping vlan 10 bridge 1
(config)#no ip dhcp snooping vlan 10 bridge 1
```

renew ip dhcp snooping binding database

Use this command to populate the binding table by fetching the binding entries from persistent storage.

Command Syntax

```
renew ip dhcp snooping (source|) binding database bridge <1-32>
```

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#renew ip dhcp snooping binding database bridge 1
```

show debugging ip dhcp snooping

Use this command to display the enabled debugging options.

Command Syntax

```
show debugging ip dhcp snooping
```

Parameters

None

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ip dhcp snooping
DHCP snoop debugging status:
DHCP snoop event debugging is on
DHCP snoop tx debugging is on
```

show ip dhcp snooping

Use this command to display the DHCP configuration, including trusted ports, rate limit, configured VLAN, active VLAN, and strict validation status.

Command Syntax

```
show ip dhcp snooping bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Rate limit(pps)                                       : 100

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
xe1/4                   Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------
```

show ip dhcp snooping arp-inspection statistics

Use this command to display the dhcp snooping dynamic ARP inspection statistics information.

Command Syntax

```
show ip dhcp snooping arp-inspection statistics bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip dhcp snooping arp-inspection statistics bridge 1

bridge      forwarded  dai dropped
------      ---------  -----------
1           0          0
```

Table 4-7 explains the show command output fields.

Table 4-7: show ip dhcp snooping arp-inspection statistics output

Field	Description
bridge	The bridge identifier (number) on which snooping is being used.
forward	Number of packets forwarded to neighbor.
dai dropped	Number of packets that have been dropped because they did not pass dynamic arp inspection (DAI).

show ip dhcp snooping binding

Use this command to display the dhcp snooping binding table.

Command Syntax

```
show ip dhcp snooping (source|) binding bridge <1-32>
```

Parameters

<1-32>	Bridge number
source	DHCP snooping IP source guard

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
# show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                : 1
Total number of dynamic IPV4 entries               : 0
Total number of static IPV6 entries                : 0
Total number of dynamic IPV6 entries               : 0

MacAddress          IpAddress      Lease(sec)     Type        VLAN    Interface
--------------    -------------    ----------  -----------    ----    ----------
0001.0002.0003      12.0.0.1           0         static        2       xe2
```

Table 4-8 explains the show command output fields.

Table 4-8: show ip dhcp snooping binding output details

Entry	Description
Total number of static IPV4 entries	Number of static IPV4 entries in the interface.
Total number of dynamic IPV4 entries	Number of dynamic IPV4 entries in the interface.
Total number of static IPV6 entries	Number of static IPV6 entries in the interface.
Total number of dynamic IPV6 entries	Number of dynamic IPV6 entries in the interface.
Mac Address	MAC address forwards the packet into a given dhcp instance.
IP Address	IP address of the peer device.
Lease (sec)	The DHCP lease time in seconds provided to untrusted IP addresses.
Type	Configured either statically or dynamically by the DHCP server.

Table 4-8: show ip dhcp snooping binding output details (Continued)

Entry	Description
VLAN	Identifier of the number.
Interface	Interface is being snooped.

CHAPTER 5 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 5-9 explains the output fields.

Table 5-9: 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 5-9: 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 6 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.

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 7 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.

Command Syntax

```
show ssh key
```

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 kedar 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 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`	VPN routing/forwarding instance.
`NAME`	Name of the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance.

Default

The default destination port 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 an 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`	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`	VPN routing/forwarding instance.
`NAME`	Name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance.

Default

The default destination port is 22.

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 server algorithm encryption

Use this command to set an encryption algorithm for SSH sessions.

An SSH server authorizes connection of only those algorithms from the list below. If a client tries to establish a connection to the server with the algorithm encryption not in the list, the connection fails.

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

Use the `no` form of this command to not encrypt SSH sessions.

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 management`	Management VPN routing/forwarding instance.

Default

No encryption.

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 <768-2048> (vrf management|)
ssh key rsa length <768-2048> 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`	Management VPN routing/forwarding instance.
`force`	Force the replacement of an SSH key
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`<768-2048>`	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
```

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`	Management VPN routing/forwarding instance.

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`	Management VPN routing/forwarding instance.

Default

By default, the 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 create a user account.

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 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 create a user account.

Command Syntax

```
username USERNAME keypair rsa
username USERNAME keypair dsa
username USERNAME keypair rsa length <768-2048>
username USERNAME keypair rsa length <768-2048> 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
`<768-2048>`	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 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)#username fred keypair rsa
```

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 <1-65535> md5 WORD (vrf management|)
ntp authentication-key <1-65535> md5 WORD 7 (vrf management|)
no ntp authentication-key <1-65535> md5 WORD (vrf management|)
```

Parameters

`<1-65535>`	Authentication key
`WORD`	MD5 string (maximum 8 characters)
`7`	Encrypt using weak algorithm
`management`	Virtual Routing and Forwarding name

Default

The default authentication key is 65535.

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 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 Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#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

```
#show ntp authentication-keys
--------------------------
 Auth Key       MD5 String
--------------------------
123             0xa2cb891442844220
```

Table 8-10 explains the output fields.

Table 8-10: 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

```
#show 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 8-11 explains the output fields.

Table 8-11: 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.
poll	The polling interval (seconds).

Table 8-11: show ntp peer-status fields

Entry	Description
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 8-12 explains the output fields.

Table 8-12: 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 8-13 explains the output fields.

Table 8-13: 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 8-14 explains the output fields.

Table 8-14: 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

```
#show 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 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:

add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

Command Syntax

```
add policy POLICY-NAME
no add policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Name of the policy

Default

None

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#no add policy myPolicy2
```

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+
```

default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Command Syntax

```
default (permit-all | deny-all)
```

Parameters

`permit-all`	Permit all commands
`deny-all`	Deny all commands

Default

Unless you explicitly give this command, the default rule for a role is `deny-all`.

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a deny rule from an RBAC policy.

Command Syntax

```
deny RULE-STRING (mode MODE-NAME |)
no deny RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)’. Deny access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#deny “ip address” mode (config-if)
```

feature dynamic-rbac enable

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the `no` form of this command to disable the RBAC feature.

Command Syntax

```
feature dynamic-rbac enable
no feature dynamic-rbac enable
```

Parameters

None

Default

By default, feature TACACS+ RBAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#feature dynamic-rbac enable
```

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
```

permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

Command Syntax

```
permit RULE-STRING (mode MODE-NAME |)
no permit RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)”. Permit access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit “ip address” mode (config-if)
```

policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

Command Syntax

```
policy POLICY-NAME
no policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Policy name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit "ip address" mode (config-if)
```

role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

Command Syntax

```
role ROLE-NAME
no role ROLE-NAME
```

Parameters

`ROLE-NAME`	Role name.
	You *cannot* specify one of these roles already defined in OcNOS:
	`network-admin`
	`network-user`
	`network-operator`
	`network-engineer`
	For more about these built-in roles, see username.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

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 rbac-policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

Command Syntax

```
show rbac-policy (POLICY-NAME |)
```

Parameters

POLICY-NAME	Policy name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#show rbac-policy myPolicy
```

show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

Command Syntax

```
show rbac-role (ROLE-NAME |)
```

Parameters

ROLE-NAME	Role name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#show rbac-role myRole
```

Table 9-15 explains the output fields.

Table 9-15: show rbac-role fields

Entry	Description
Role Name	Role name
Default rule	permit-all or deny-all
Attached Policies	Name of policies attached to this role

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

```
#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 7
0x9f4a8983e0216052
```

Table 9-16 explains the output fields.

Table 9-16: 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 9-17 explains the output fields.

Table 9-17: 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 9-17: 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
```

CHAPTER 10 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 VRFs

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS version 1.3.7.

Examples

```
#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|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
  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>)|) acctport <0-65535> |) | timeout <1-60> |)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) 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
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`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 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>)|) (|(authport <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|)
  (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|) (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).

Command Syntax

```
radius-server login timeout <1-60> (vrf management|)
no radius-server login timeout (vrf management|)
```

Parameters

`login`	Remote login
`<1-1000>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

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 10-18 explains the output fields.

Table 10-18: 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
radius-server login key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb vrf management
radius-server login host 10.12.12.39 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
```

CHAPTER 11 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 11-19 explains the output fields.

Table 11-19: 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 11-20 explains the output fields.

Table 11-20: 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. You do not specify an engine identifier for a device; OcNOS generates a default string.

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 11-21 explains the output fields.

Table 11-21: 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 11-22 explains the output fields.

Table 11-22: 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 11-23 explains the output fields.

Table 11-23: 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 SNMP traps and inform requests.

Use `no` form of this command to disable SNMP traps and inform requests.

Command Syntax

```
snmp-server enable traps (link(|linkDown|linkUp)|snmp(|authentication)|
  mpls|pw|pwdelete|rsvp|ospf|bgp|isis)
no snmp-server enable traps (link(|linkDown|linkUp)|snmp(|authentication)|
  mpls|pw|pwdelete|rsvp|ospf|bgp|isis)
```

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
`mpls`	Enable notification trap for MPLS
`pw`	Enable notification trap for pseudowire
`pwdelete`	Enable notification trap for pseudowire delete
`rsvp`	Enable notification trap for RSVP
`ospf`	Enable notification trap for OSPF
`bgp`	Enable notification trap for BGP
`isis`	Enable notification trap for ISIS

Default

By default, SNMP server traps are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.6.

Examples

```
(config)#snmp-server enable traps snmp authentication
(config)#sh running-config snmp
snmp-server view all .1 included vrf management
snmp-server enable snmp vrf management
snmp-server enable traps snmp authentication
```

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 12 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 10, *RADIUS*
- Chapter 9, *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 console
- 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 accounting
- show aaa groups
- 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 console

Use this command to set the AAA authentication methods for console log ins.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login console ((group LINE) | (local (|none)) | (none))
no aaa authentication login console ((group LINE) | (local (|none)) | (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	Specify 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

Default

Default AAA authentication 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 authentication login console 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 console fallback error

Use this command to enable fallback to local authentication for the console 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 console fallback error local
no aaa authentication login console fallback error local
```

Parameters

None

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 console fallback error local
```

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.

Note: If you have specified `local` (use local authentication) in the aaa authentication login default command, you do not need to use this command to ensure that “fall back to local” occurs.

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 configuration 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 12-24 explains the output fields.

Table 12-24: show aaa authentication fields

Entry	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
```

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
```

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
```

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 12-25 explains the output fields.

Table 12-25: show aaa accounting fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.

CHAPTER 13 Configuration 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 13-26 to remotely transfer files:

Table 13-26: 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 http startup-config (interactive)
- copy ftp startup-config (interactive)
- copy scp startup-config (interactive)
- copy sftp running-config (interactive)
- copy tftp startup-config (interactive)
- copy http startup-config (interactive)
- copy startup-config running-config
- copy file running-config
- copy file startup-config

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
#
```

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) 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`	Techsupport file storage; on Linux this refers to `/var/log/`
`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 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) FILE (ftp|tftp|scp|sftp) (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`	Techsupport file storage; on Linux this refers to `/var/log/`
`FILE`	Source file name
`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 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 ftp running-config

Use this command to append the running configuration from an FTP server to the local device.

Command Syntax

```
copy ftp FTP-URL running-config append (store|) (vrf (NAME|management)|)
```

Parameters

`FTP-URL`	Configuration source: `ftp:[//server][/path]`
`store`	Store the running-configuration
`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 running-config appen store 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 scp running-config

Use this command to append the running configuration from an SCP server to the local device.

Command Syntax

```
copy scp SCP-URL running-config append (store|) (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `SCP:[//server][/path]`
`store`	Store the running configuration
`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 running-config appen store 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 sftp running-config

Use this command to append the running configuration from an SFTP server to the local device.

Command Syntax

```
copy sftp SFTP-URL running-config append (store|) (vrf (NAME|management)|)
```

Parameters

SFTP-URL	Configuration source: sftp:[//server][/path]
store	Store the running-configuration
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/sftp filename running-config appen store 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 tftp running-config

Use this command to append the running configuration from an FTP server to the local device.

Command Syntax

```
copy tftp TFTP-URL running-config append (store|) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Configuration source: `tftp:[//server][/path]`
`store`	Store the running-configuration
`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 running-config appen store 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 http running-config

Use this command to append the running configuration from an HTTP server to the local device.

Command Syntax

```
copy http HTTP-URL running-config append (store|) (vrf (NAME|management)|)
```

Parameters

`HTTP-URL`	Configuration source: `http:[//server][/path]`
`store`	Store the running-configuration
`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 running-config appen store vrf
management
```

copy scp running-config (interactive)

Use this command to copy and store the running configuration from an SCP server to the local device.

Command Syntax

```
copy scp running-config (append|) store (vrf (NAME|management)|)
```

Parameters

`append`	Append the configuration into running-config
`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 running-config append store vrf management
```

copy sftp running-config (interactive)

Use this command to copy and store the running configuration from an SFTP server to the local device.

Command Syntax

```
copy sftp running-config (append|) store (vrf (NAME|management)|)
```

Parameters

`append`	Append the configuration into running-config
`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 running-config append store vrf management
```

copy tftp running-config (interactive)

Use this command to copy and store the running configuration from a TFTP server to the local device.

Command Syntax

```
copy tftp running-config (append|) store (vrf (NAME|management)|)
```

Parameters

`append`	Append the configuration into running-config
`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 running-config append store vrf management
```

copy http running-config (interactive)

Use this command to copy and store the running configuration from an HTTP server to the local device.

Command Syntax

```
copy http running-config (append|) store (vrf (NAME|management)|)
```

Parameters

`append`	Append the configuration into running-config
`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 running-config append store 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 startup-config running-config

Use this command to copy the start-up configuration to the running configuration.

Command Syntax

```
copy startup-config running-config
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config running-config
```

copy file running-config

Use this command to copy and store a file into the running configuration.

Command Syntax

```
copy file FILE running-config (append|) store
```

Parameters

`FILE`	File name
`append`	Append the configuration into running-config
`store`	Store configuration

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy file myFile running-config append store
```

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 14 Software Monitoring and Reporting

This document describes software watchdog and reporting related commands.

copy techsupport

Use this command to copy the contents of a compressed techsupport file (`tar.gz`) to another file.

The default filename is in the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

Syntax

```
copy (log|techsupport) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL)
  (vrf (NAME|management)|)
```

Parameters

`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Tech support file storage; on Linux this refers to `/var/log/`
`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

Default

NA

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy techsupport tech_support_23_Feb_2019_18_27_00.tar.gz scp scp://10.12.16.17/home/
tech_support_23_Feb_2019_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
#
```

feature software-watchdog

Use this command to enable software watchdog functionality for all OcNOS modules. This feature is enabled by default.

Use the `no` form of this command to disable software watchdog functionality.

Command Syntax

```
feature software-watchdog
```

```
no feature software-watchdog
```

Parameter

None

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)feature software-watchdog
```

show bootup-parameters

Use this command to show OcNOS kernel bootup parameters.

Command Syntax

```
show bootup-parameters
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bootup-parameters
BOOT_IMAGE=/boot/vmlinuz-3.16.7-g490411a-ec-as7712-32x root=UUID=317567fc-
b69e-4

5d9-ab4e-fa1d9e57b

703 console=ttyS1,115200n8 ro
```

show cores

Use this command to list core files in the system or to display information about a given core file.

Command Syntax

```
show cores (|WORD details)
```

Parameter

WORD	Core file name

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh cores
Core location :/var/log/crash/cores
Core-File-Name
--------------
core_nsm.683_20191110_103611_signal_5.gz
core_nsm.712_20191107_171803_signal_11.gz
core_nsm.684_20191112_054937_signal_5.gz
core_yangcli.5695_20191107_171715_signal_11.gz
#
```

Table 14-27 explains the output fields.

Table 14-27: show cores fields

Entry	Description
Core-File-Name	Core dump file name.

show software-watchdog status

Use this command to display the software watchdog status for each OcNOS module.

Command Syntax

```
show software-watchdog status
show software-watchdog status detail
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.4.

Examples

```
#show software-watchdog status
Software Watchdog timeout in seconds : 60
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ripngd               Enabled
ospfd                Enabled
ospf6d               Enabled
isisd                Enabled
hostpd               Enabled
ldpd                 Enabled
rsvpd                Enabled
mribd                Enabled
pimd                 Enabled
authd                Enabled
mstpd                Enabled
imi                  Enabled
onmd                 Enabled
HSL                  Enabled
oamd                 Enabled
vlogd                Enabled
vrrpd                Enabled
ndd                  Enabled
ribd                 Enabled
bgpd                 Enabled
l2mribd              Enabled
lagd                 Enabled
sflow                Enabled
```

```
cmld                  Enabled
cmmd                  Enabled

#show software-watchdog status detail
Software Watchdog timeout in seconds : 60

Process Watchdog   Process   Disconnect Connect         Last Restart
 Name    Status     Status     Count     Count             Reason
======= ======== =========== ========== ======= ==============================
nsm     Enabled  Running     0          1       Fresh bootup
ripd    Enabled  Running     0          1       Fresh bootup
ripngd  Enabled  Running     0          1       Fresh bootup
ospfd   Enabled  Running     0          1       Fresh bootup
ospf6d  Enabled  Running     0          1       Fresh bootup
isisd   Enabled  Running     0          1       Fresh bootup
hostpd  Enabled  Running     0          1       Fresh bootup
ldpd    Enabled  Running     0          1       Fresh bootup
rsvpd   Enabled  Running     0          1       Fresh bootup
mribd   Enabled  Running     0          1       Fresh bootup
pimd    Enabled  Running     0          1       Fresh bootup
authd   Enabled  Running     0          1       Fresh bootup
mstpd   Enabled  Running     0          1       Fresh bootup
imi     Enabled  Running     0          1       Fresh bootup
onmd    Enabled  Running     0          1       Fresh bootup
HSL     Enabled  Running     0          1       Fresh bootup
oamd    Enabled  Running     0          1       Fresh bootup
vlogd   Enabled  Running     0          1       Fresh bootup
vrrpd   Enabled  Running     0          1       Fresh bootup
ndd     Enabled  Running     0          1       Fresh bootup
ribd    Enabled  Running     0          1       Fresh bootup
bgpd    Enabled  Running     0          1       Fresh bootup
l2mribd Enabled  Running     0          1       Fresh bootup
lagd    Enabled  Running     0          1       Fresh bootup
sflow   Enabled  Running     0          1       Fresh bootup
cmld    Enabled  Running     0          1       Fresh bootup
cmmd    Enabled  Running     0          1       Fresh bootup
```

Table 14-28 explains the output fields.

Table 14-28: show software-watchdog status output fields

Field	Description
Process Name	The name of a protocol module.
Watchdog Status	Status of a protocol module (Enabled or Disabled).
Process Status	Status of the protocol module Running/Not-running).
Disconnect Count	Number of times the protocol module disconnected from monitoring module.

Table 14-28: show software-watchdog status output fields (Continued)

Field	Description
Connect Count	Number of times the protocol module connected to monitoring module.
Last Restart Reason	Reason why a module disconnected from monitoring module.

show system log

Use this command to display the system's log file.

Command Syntax

```
show system log
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system log
Syslog              : enabled      File Name    : /var/log/messages
Oct 18 18:10:18 localhost rsyslogd: [origin software="rsyslogd"
swVersion="8.4.2
" x-pid="541" x-info="http://www.rsyslog.com"] start
Oct 18 18:10:18 localhost systemd[1]: Started Apply Kernel Variables.
Oct 18 18:10:18 localhost systemd[1]: Started Create Static Device Nodes in /
dev
.
Oct 18 18:10:18 localhost systemd[1]: Starting udev Kernel Device Manager...
Oct 18 18:10:18 localhost systemd[1]: Started udev Kernel Device Manager.
Oct 18 18:10:18 localhost systemd[1]: Starting Copy rules generated while the
ro
ot was ro...
Oct 18 18:10:18 localhost systemd[1]: Starting LSB: Set preliminary keymap...
Oct 18 18:10:18 localhost systemd[1]: Started Copy rules generated while the
roo
t was ro.
Oct 18 18:10:18 localhost nfs-common[163]: Starting NFS common utilities:.
Oct 18 18:10:18 localhost systemd[1]: Found device /dev/ttyS0.
Oct 18 18:10:18 localhost systemd[1]: Found device 16GB_SATA_Flash_Drive
OcNOS-CONFIG.
Oct 18 18:10:18 localhost systemd[1]: Starting File System Check on /dev/disk/
by
-label/OcNOS-CONFIG...
Oct 18 18:10:18 localhost systemd[1]: Starting system-ifup.slice.
Oct 18 18:10:18 localhost systemd-fsck[217]: OcNOS-CONFIG: clean, 85/128016
file
s, 27057/512000 blocks
Oct 18 18:10:18 localhost systemd[1]: Created slice system-ifup.slice.
--More--
```

Table 14-29 explains the output fields.

Table 14-29: show system log fields

Entry	Description
Syslog	Status of the protocol (enabled or disabled).
File Name	Specifies the name of the system log files that you configured.

show system login

Use this command to display the system's login history.

Command Syntax

```
show system login
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system login
eric      ttyS0                        Wed Oct 19 18:31   still logged in
takayuki  ttyS0                        Wed Oct 19 18:14 - 18:25  (00:10)
girish    ttyS0                        Wed Oct 19 16:46 - 17:01  (00:14)

wtmp begins Wed Oct 19 16:46:18 2016
```

show system reboot-history

Use this command to show the OcNOS reboot history.

Command Syntax

```
show system reboot-history
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show system reboot-history
#) On Thu Jun 6 06:16:03 2013
Reason: Reset Requested by Active User
Service: NONE
#) On Thu Jun 6 06:21:30 2015
Reason: Reset Requested due to Process Crash
Service: nsm
#
```

Table 14-29 explains the output fields.

Table 14-30: show system reboot-history fields

Entry	Description
Reason	Displays the reason, why the fields are reset.
Service	Name of the service in this protocol.

show system resources

Use this command to display the system's current resources.

Command Syntax

```
show system resources (iteration <1-5>|)
```

Parameters

<1-5>	The number of times to check the resources before they are displayed.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system resources
load average: 0.11, 0.08, 0.05
Tasks: 113 total,   1 running, 112 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.1 us,  0.4 sy,  0.0 ni, 98.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
KiB Mem:   8181040 total,   736124 used,  7444916 free,   133012 buffers


#show system resources iteration 5
load average: 0.03, 0.06, 0.05
Tasks: 112 total,   3 running, 109 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  0.6 sy,  0.0 ni, 98.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
KiB Mem:   8181040 total,   736608 used,  7444432 free,   132976 buffers
KiB Swap:        0 total,        0 used,        0 free.   252416 cached Mem
```

Table 14-31 explains the output fields.

Table 14-31: show system resource fields

Entry	Description
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.
Tasks	Number of processes in the system and how many processes are actually running when the command is issued.
CPU	Displays the CPU utilization information for processes on the device.

Table 14-31: show system resource fields

Entry	Description
KiB Mem	The memory field (Mem) shows the virtual memory used by processes. The value in the memory field is in KB and MB, and is broken down as follows: Total: The total amount of available virtual memory, in kibibytes (KiBs). Used:The total amount of used virtual memory, in kibibytes (KiBs). Free: The total amount of free virtual memory, in kibibytes (KiBs) Buffers: The size of the memory buffer used to hold data recently called from disk.
KiB Swap	The Swap field shows the total swap space available and how much is unused and is broken down as follows: Total: The total amount of available swap memory, in kibibytes (KiBs). Used: The total amount of used swap memory, in kibibytes (KiBs). Free: The total amount of free swap memory, in kibibytes (KiBs). Cache Memory: Memory that is not associated with any program and does not need to be swapped before being reused.

show system uptime

Use this command to display how lone the system has been up and running.

Command Syntax

```
show system uptime
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system uptime
 19:10:22 up 1 day,  1:01,  1 user,  load average: 0.08, 0.05, 0.05
```

Table 14-32 explains the output fields.

Table 14-32: show system uptime fields

Entry	Description
Time and up	Current time, in the local time zone, and how long the router or switch has been operational.
Users	Number of users logged in to the router or switch.
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.

show techsupport

Use this command to collect system data for technical support to save support information in a compressed (.gz) file.

The default file path is `/var/log/` and the filename is `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

The filename given can be the same as another file; to distinguish them, each of the filenames are appended with a date and timestamp.

If a `show techsupport` command execution is in progress, any newly issued `show techsupport` commands are ignored.

If a `show techsupport` command is executing, and the `show running-config` command is given, the displayed information is copied from the `show techsupport` command.

Command Syntax

```
show techsupport
  ({bgp|authd|isis|lag|ldp|mstp|ospf|pim|hostpd|hsl|l2mribd|mribd|nsm|oam|onm|osp6
  |rib|ripng|sflow|vrrp|rip|rsvp|imi|trill|all|cmmd})(log-path WORD)(status)
```

Parameters:

`daemon`	Protocol/daemon name
`WORD`	The path and filename (log-path) where the technical support information is saved.
`status`	Displays the status of the completion of the technical support `tar_.gz` file.
`all`	Include all protocol information in the technical support `tar_.gz` file.

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 techsupport all
#show techsupport all log-path /home/filename
#show techsupport nsm
#show techsupport nsm log-path /home/filename
#show techsupport hostpd authd imi
#show techsupport hostp authd imi log-path /home/filename
#show techsupport status
```

software-watchdog

Use this command to enable the software watchdog feature for an OcNOS module.

Use the `no` form of this command to disable the software watchdog feature.

Command Syntax

```
software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd||
  ldpd|rsvpd||trilld|hsl|cmmd)
no software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd||
  ldpd|rsvpd||trilld|hsl|cmmd)
```

Parameters

`nsm`	NSM module
`authd`	AUTH module
`bgpd`	BGP module
`cmld`	CML module
`hostpd`	HOSTP module
`imi`	IMI module
`isisd`	ISIS module
`lagd`	LAG module
`l2mribd`	L2MRIB module
`mstpd`	MSTP module
`mribd`	MRIB module
`ndd`	NDD module
`oamd`	OAM module
`onmd`	ONM module
`ospfd`	OSPF module
`ospf6d`	OSPF6 module
`pimd`	PIM module
`ribd`	RIB module
`ripd`	RIP module
`ripngd`	RIPNG module
`sflow`	SFLOW module
`vlogd`	VLOG module
`vrrpd`	VRRP module
`ldpd`	LDP module
`rsvpd`	RSVP module
`trilld`	TRILL module

`hsl`	HSL module
`cmmd`	CMM module

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)no software-watchdog imi
#(config)software-watchdog nsm
```

software-watchdog keep-alive-time

Use this command to set the software watchdog keep-alive time interval in seconds. The default keep-alive time interval is 60 seconds.

Use the `no` form of this command to set default keep-alive time interval.

Command Syntax

```
software-watchdog keep-alive-time <30-1800>
no software-watchdog keep-alive-time
```

Parameters

`<30-1800>`	Keep-alive time interval in seconds

Default

By default, software watchdog is enabled and the keep-alive time interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)software-watchdog keep-alive-time 100
```

CHAPTER 15 Interface Commands

This chapter is a reference for each of the interface commands.

- show flowcontrol
- show flowcontrol
- show interface
- show interface capabilities
- 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 summary
- show interface fec
- 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
- show running-config prefix-list
- 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 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.

This command is not available on Qumran platforms.

Example

```
#clear interface cpu counters
```

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
```

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 before 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 up to 128 characters.

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`.

```
#configure terminal
(config)#interface eth1
(config-if)#description Connected to Zenith's fas2/0
```

duplex

Use this command to set the duplex mode for an 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, the duplex mode is full.

Note: The `duplex half` option is supported only up to 100M. When speed is in auto mode, duplex properties are negotiated. For 1G speeds and beyond, only full duplex speeds are negotiated.

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 set forward error correction (FEC) on a physical port.

In “force speed" mode, FEC configuration should be same on both peers, otherwise the interface will be down. Giving the “`fec auto`” command does not enable FEC when the interface is in "force speed" mode.

Only use "`fec auto`" with "speed auto" mode. Force setting FEC in "speed auto" mode does not change the FEC status.

Use the no form of this command to remove FEC.

Command Syntax

```
fec (on|auto)
no fec
```

Parameter

`on`	Enable FEC.
`auto`	Enable FEC with auto negotiation.

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
```

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

Flow control is disabled by default. If auto-negotiation is off or if the port speed was configured manually, flow control is not negotiated and is not advertised to the peer. Verify this by checking the OPER status of flow control using show flowcontrol command:

- If the interface is in speed auto mode and flow control is enabled on both peers, the OPER status is ON.
- If flow control is configured when the interface is in speed force mode, flow control is not negotiated with the peer. The OPER status will be ON right after the configuration.

Note: Configuring flow control flaps the interface.

To change speed settings, see the speed command.

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-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 using this command to enter 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 local-proxy-arp

Use this command to enable local proxying of ARP requests at the interface level.

After giving this command, the device answers all ARP requests on a configured subnet, even for clients that normally do not need routing. Local proxy ARP implies a proxy ARP that occurs on the same interface, that is, the traffic comes in and goes out the same interface.

With local proxy ARP, 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.

Use the `no` parameter to disable the local proxy ARP feature on an interface.

Command Syntax

```
ip local-proxy-arp
no ip local-proxy-arp
```

Parameters

None

Default

By default, local 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 local-proxy-arp
```

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.

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 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
```

mtu

Use this command to set the Maximum Transmission Unit (MTU) 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 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,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

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
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


ethernet cfm enable
!
interface ce1/1
port breakout enable 4X25g
```

Similarly, a 100G port can be split into 4x10G ports or 2x50G ports.

show flowcontrol

Use this command to display flow control information.

Command Syntax

```
show flowcontrol
show flowcontrol interface IFNAME
```

Parameters

`IFNAME`	The name of an interface.

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 15-33 explains the show command output fields.

Table 15-33: 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

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 15-34 explains the output fields.

Table 15-34: 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 capabilities

Use this command to display interface capabilities

Command Syntax

```
show interface (IFNAME|) capabilities
```

Parameters

IFNAME	The name of an interface.

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 15-35 explains the show command output fields.

Table 15-35: 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 15-35: 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.

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.

This command is not available on Qumran platforms.

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 15-36 explains the output fields.

Table 15-36: show interface counters output details

Field	Description
Receive Counters	Rx Packets Rx Bytes Rx Unicast Packets Rx Packets from 128 to 255 bytes Rx Discard Packet
Transmit Counters	Tx Packets Tx Bytes Tx Multicast Packets Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes
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.

This command is not available on Qumran platforms.

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 15-37 explains the output fields.

Table 15-37: 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.
Rx Vlan Discards	VLAN received packets dropped because there is no VLAN configured on the port.
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.
Rx Policy Discards	Received packets dropped because of device policies violated, such as a storm control rate violation.
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: 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 In static MAC movement, a source MAC address is configured in hardware as a static entry. This counter does not increment for static MAC movement if `watch static-mac-movement` is configured, and is reflected in the `l2-movement` queue statistics.
Rx IBP Discards	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface.
Tx Port Block Drops	Transmitted packets dropped because port blocking is enabled.

Table 15-37: show interface counters drop-stats output details (Continued)

Field	Description
Tx Vlan Discards	Transmitted VLAN packets dropped because there is no VLAN configured on the port.
Tx TTL Discards	Transmitted packets discarded because their Time To Live (TTL) has ended.
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.
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 15-38 explains the columns in the output.

Table 15-38: 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 15-39 explain the fields in the command output.

Table 15-39: 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: • 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
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: • 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 • Source MAC is configured as static on other interface • 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 15-40 explain the fields in the command output.

Table 15-40: 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.

Table 15-40: outdiscard statistics

Statistics	Description
TTL Discards	Packets discarded because the Time-To Live (TTL) of the outgoing packet has passed.
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 15-41 explain the fields in the command output.

Table 15-41: 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.

This command is not available on Qumran platforms.

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 15-42 explain the fields in the command output.

Table 15-42: 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.

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.

This command is not available on Qumran platforms.

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 15-43 explain the fields in the command output.

Table 15-43: 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 15-44 explain the fields in the command output.

Table 15-44: 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.

This command is not available on Qumran platforms.

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 15-45 explain the fields in the command output.

Table 15-45: 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 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 15-46 explain the fields in the command output.

Table 15-46: 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 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 15-47 explain the fields in the command output.

Table 15-47: 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 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 15-48 explain the fields in the command output.

Table 15-48: 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 15-49 explain the fields in the command output.

Table 15-49: 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 15-49: 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 15-50 shows these codes and modifiers.

Table 15-50 explain the fields in the command output.

Table 15-50: 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 15-51 explains the each route entry fields.

Table 15-51: route entry output details

Field	Description
Codes and modifiers	As explained in Table 15-50.
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 15-50.

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.

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 15-52 explains the each interface brief entry.

Table 15-52: 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 15-50 and Table 15-51 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 15-53 explains the output fields.

Table 15-53: 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 15-53: 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 dot1x
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
show running-config interface IFNAME trill
```

Parameters

`bridge`	Bridge.
`dot1x`	IEEE 802.1X port-based access control.
`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.
`trill`	Transparent Interconnection of Lots of Links.

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
!
```

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
!
```

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 to use auto speed on such transceivers. On DAC cables, both force and auto negotiation are supported.

IP Infusion Inc. recommends to configure same speed mode on both the peers.

On Trident2 and Trident2+ switches, even if a fiber port is running at a variable 10M/100M/1G auto-negotiated speed, if you give this command to manually set the speed to less than 1G, the speed is always set to 1G. However, the show interface command displays the speed of such ports as set by you.

If the speed of the optic connected is less than the front-panel port capability and you force the speed to the front panel port capability, the interface might come up. For example, on a 100g front panel port, if you insert 40g optics and force the speed to 100g, the interface might come up in 100g speed.

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 interface does not come up in auto mode. To bring the interface up, 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 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 negotiation at the 1g speed and the port will come up.

Note: For 10 DAC/AOC, setting `speed auto` negotiates with a maximum of 1G.

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

Configure forced speed to 10G:

```
#configure terminal
(config)#interface xe0
(config-if)#speed 10g
```

Enable auto-negotiation:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto
```

Enable auto-negotiation up to 10G:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto 10g
```

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.

Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```

CHAPTER 16 Access Control List Commands (XGS)

This chapter is a reference for the Access Control List (ACL) commands for XGS devices (Trident II, Trident II+, and Tomahawk):

- mac access-list
- mac access-list default
- mac access-list filter
- mac access-list remark
- mac access-list resequence
- show access-lists
- show access-list log-cache
- show arp access-lists
- show ip access-lists
- show ipv6 access-lists
- show mac access-lists
- show running-config aclmgr
- show running-config access-list
- show running-config ipv6 access-list

access-list logging cache-size

Use this command to set the ACL logging table size.

Use the `no` form of this command to set the table size to its default (1000).

Command Syntax

```
access-list logging cache-size <1000-10000>
no access-list logging cache-size
```

Parameters

`<1000-10000>`	Maximum number of cache entries

Default

By default, the logging table size is 1000.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list logging cache-size 2000
(config)#end
```

access-list logging rate-limit

Use this command to set the rate limit for logging ACL denied packets.

Use the `no` form of this command to reset the rate to its default (200).

Command Syntax

```
access-list logging rate-limit <0-1000>
no access-list logging rate-limit
```

Parameters

`<0-1000>`	Packets per second

Default

By default, the rate is 200 packets per second.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list logging rate-limit 500
(config)#end
```

arp access-group

Use this command to attach ARP access list to an interface to filter incoming ARP 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 ARP access group.

Note: To attach an ARP access-group to an interface, the ingress-arp TCAM group should be enabled. See the hardware-profile filter (XGS) command for more 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 version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#interface xe1
(config-if)#arp access-group ARP_ACL1 in
(config-if)#no arp access-group ARP_ACL1 in
```

arp access-list

Use this command to define a named ARP access control list (ACL) that determines whether to accept or drop an incoming ARP packet based on the sender or target IP address, sender or target MAC address, ARP type.

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 sequenced. 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. The implied specification can be updated to permit if the use-case is to deny a certain set of ARP traffic.

Use the no form of this command to remove an ACL specification

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 version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#no arp access-list ARP_ACL1
```

arp access-list filter

Use this command to configure access control entry in ARP access control list (ACL).

This determines whether to accept or drop an ARP 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 results in an update of 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-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
  XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
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-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
  XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	ARP ACL sequence number.
`request`	RP request type
`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`	Single source host IP address.
`any`	Match any source IP address.
`any`	Any source/destination.
`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).

`vlan <1-4094>` VLAN identifier.

`inner-vlan<1-4094>`
: Inner VLAN identifier.

`log` Log the packets matching the filter (in-direction only).

`sample` Sample the packets matching the filter (in-direction only).

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#15 permit ip host 2.2.2.1 mac any inner-vlan 3
(config-arp-acl)#no 15
```

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 version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list arplist
(config-arp-acl)#remark permit the selected arp entries
(config-arp-acl)#exit
(config)#arp access-list arplist
(config-arp-acl)#no remark
(config-arp-acl)#exit
```

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.

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 version 1.3.6.

Example

```
#configure terminal
(config)#ip access-list arplist
(config-arp-acl)#resequence 5 5
(config-arp-acl)#end
```

arp access-list response

Use this command to configure an ARP access control entry in an ARP access control list (ACL). This 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.

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-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
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-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	ARP ACL sequence number.
`response`	ARP reply type
`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.

`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 (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.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#50 permit response ip host 2.2.2.1 any mac any any vlan 2
(config-arp-acl)#no 50 permit response ip host 2.2.2.1 any mac any any vlan 2
```

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 access-list log-cache

Use this command to clear the access-list logging table.

Command Syntax

```
clear access-list log-cache
```

Parameters

None

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear access-list log-cache
```

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 version 1.3.6.

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.

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 version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#interface eth3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface eth3
(config-if)#no ip access-group mylist in
(config-if)#exit
```

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, ensure the `ingress-ipv4` TCAM group is enabled. See the hardware-profile filter (XGS) commands for details.

Usage: Loopback and VTY Interfaces

You can create ACLs for loopback (inband) and VTY interfaces to protect management applications such as SSH, Telnet, NTP, SNMP, and SNMP traps. Filtering TCP, UDP, and ICMP are supported.

Note: Loopback and VTY ACLs are mutually exclusive. If you set up one, you cannot set up the other.

For an ACL for a loopback interface, you create the ACL, configure it with rules, and associate the ACL with a loopback interface:

```
...
(config)#interface lo
(config-if)#ip access-group loopback in
```

For an ACL for VTY, you create the ACL, configure it with rules, and associate the ACL to the terminal line in line mode:

```
...
(config)#line vty
(config-all-line)#ip access-group vty in
```

Loopback and 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.

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.

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) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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 sample
```

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 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) (<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 )|) (fragments|) (vlan <1-4094>|)(inner-vlan <1-4094>|) (log|)
  (sample|)((redirect-to-port IFNAME)|)
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 )|) (fragments|) (vlan <1-4094>|)(inner-vlan <1-
  4094>|) (log|) (sample|)|)((redirect-to-port IFNAME)|)
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`	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.
`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).
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected

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 fragments

Use this command to configure access list to deny or permit all the IP fragmented packets.

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>|) fragments (deny-all|permit-all) (log|) (sample|)
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

Parameters

`deny-all`	Drop the packet.
`permit-all`	Accept the packet.
`<1-268435453>`	IPv4 ACL sequence number.
`fragments`	Check non-initial.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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)#fragments deny-all
(config-ip-acl)#end
```

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 identifier, inner VLAN identifier, and fragment number 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) (administratively-prohibited|
  alternate-address| conversion-error|dod-host-prohibited| dod-net-prohibited|
  echo| echo-reply|general-parameter-problem| host-isolated| host-precedence-
  unreachable|host-redirect| host-tos-redirect| host-tos-unreachable| host-
  unknown|host-unreachable| information-reply| information-request| mask-
  reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
  unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
  packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
  protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
  solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
  timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
  ((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))|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|) (sample|)
  ((redirect-to-port IFNAME)|)

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) (administratively-
  prohibited| alternate-address| conversion-error|dod-host-prohibited| dod-net-
  prohibited| echo| echo-reply|general-parameter-problem| host-isolated| host-
  precedence-unreachable|host-redirect| host-tos-redirect| host-tos-unreachable|
  host-unknown|host-unreachable| information-reply| information-request| mask-
  reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
  unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
  packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
  protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
  solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
  timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
  ("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))|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)(log|)(sample|)
  ((redirect-to-port IFNAME)|)
```

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.

`administratively-prohibited`
Administratively prohibited.

`alternate-address`
Alternate address.

`conversion-error`
Datagram conversion.

`dod-host-prohibited`
Host prohibited.

`dod-net-prohibited`
Net prohibited.

`echo` Echo (ping).

`echo-reply` Echo reply.

`general-parameter-problem`
Parameter problem.

`host-isolated` Host isolated.

`host-precedence-unreachable`
Host unreachable for precedence.

`host-redirect` Host redirect.

`host-tos-redirect`
Host redirect for ToS.

`host-tos-unreachable`
Host unreachable for ToS.

`host-unknown` Host unknown.

`host-unreachable`
Host unreachable.

`information-reply`
Information replies.

`information-request`

Information requests.

`mask-reply` Mask replies.

`mask-request` Mask requests.

`mobile-redirect`
Mobile host redirect.

`net-redirect` Network redirect.

`net-tos-redirect`
Net redirect for ToS.

`net-tos-unreachable`
Network unreachable for ToS.

`net-unreachable`
Net unreachable.

`network-unknown`
Network unknown.

`no-room-for-option`
Parameter required but no room.

`option-missing` Parameter required but not present.

`packet-too-big` Fragmentation needed and DF set.

`parameter-problem`
All parameter problems.

`port-unreachable`
Port unreachable.

`precedence-unreachable`
Precedence cutoff.

`protocol-unreachable`
Protocol unreachable.

`reassembly-timeout`
Reassembly timeout.

`redirect` All redirects.

`router-advertisement`
Router discovery advertisements.

`router-solicitation`
Router discovery solicitations.

`source-quench` Source quenches.

`source-route-failed`
Source route failed.

`time-exceeded` All time-exceeded messages.

`timestamp-reply`
Time-stamp replies.

`timestamp-request`	
	Time-stamp requests.
`traceroute`	Traceroute.
`ttl-exceeded`	TTL exceeded.
`unreachable`	All unreachables.
`<0-255>`	ICMP type.
`<0-255>`	ICMP code.
`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).
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected

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.

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 the sequence numbers of an IP access list specification.

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.

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 packet based on the criteria specified match criteria.

This form of this 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.

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}|) (fragments|)(vlan <1-4094>|)(inner-vlan
  <1-4094>|)(log|) (sample|)((redirect-to-port IFNAME)|)

(<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))|)
  (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|) (sample|)

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}|) (fragments|)(vlan <1-
  4094>|)(inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)
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)) |) (fragments|)(vlan <1-4094>|)(inner-vlan <1-
  4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)
```

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>	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).
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.
`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.
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`IFNAME`	Interface name to which packet to be redirected
`redirect-to-port`	Redirect the packet (in-direction only)

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

Use this command to attach an IPv6 access list to an interface to filter incoming or outgoing 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` parameter with this command to detach an IPv6 access list.

Note: To attach an IPv6 access-group on interface, the IPv6 TCAM group should be enabled. To enable ingress-IPv6 /egress-IPv6, see the hardware-profile filter (XGS) command.

Command Syntax

```
ipv6 access-group NAME (in|out)
no ipv6 access-group NAME (in|out)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets.
`out`	Filter outgoing packets.

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)#interface eth3
(config-if)#ipv6 access-group mylist in

(config)#interface eth3
(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 an ACL.

Command Syntax

```
ipv6 access-list NAME
no ipv6 access-list NAME
```

Parameters

`NAME`	Access-list name.

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 access-list. Default rule is applicable only when 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) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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 sample
```

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

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.

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|host 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 )|) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|)(inner-vlan
  <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

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|host 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 )|) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|)(inner-vlan
  <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

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.
`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. `v`

`rrp`	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`	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 identifier.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Inner-VLAN identifier.
`redirect-to-port`	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected

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-ip-acl)#permit ipipv6 any any
(config-ip-acl)#end
```

ipv6 access-list fragments

Use this command to permit or deny all the IPv6 fragments.

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>|) fragments (deny-all|permit-all) (log|) (sample|)
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`fragments`	Check non-initial fragments.
`deny-all`	Specify packets to reject.
`permit-all`	Specify packets to forward.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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)#fragments deny-all
```

ipv6 access-list icmpv6

Use this command to permit or deny IPv6 ICMP packets with the given source and destination IPv6 address, DSCP value, VLAN identifier, inner VLAN identifier, fragments, and flow label.

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) (beyond-scope| destination-unreachable| echo-reply|
  echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
  header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
  unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
  router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
  (<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flow-
  label <0-1048575>|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|)
  (sample|)((redirect-to-port IFNAME)|)

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) (beyond-scope| destination-unreachable| echo-reply|
  echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
  header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
  unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
  router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
  (<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef )|) (flow-
  label <0-1048575>|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)(log|)
  (sample|)((redirect-to-port IFNAME)|)
```

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
`beyond-scope`	Destination beyond scope
`destination-unreachable`	

	Destination address is unreachable
`echo-reply`	Echo reply
`echo-request`	Echo request (ping)
`header`	Parameter header problems
`hop-limit`	Hop limit exceeded in transit
`mld-query`	Multicast Listener Discovery Query
`mld-reduction`	Multicast Listener Discovery Reduction
`mld-report`	Multicast Listener Discovery Report
`nd-na`	Neighbor discovery neighbor advertisements
`nd-ns`	Neighbor discovery neighbor solicitations
`next-header`	Parameter next header problems
`no-admin`	Administration prohibited destination
`no-route`	No route to destination
`packet-too-big`	Packet too big
`parameter-option`	
	Parameter option problems
`parameter-problem`	
	All parameter problems
`port-unreachable`	
	Port unreachable
`reassembly-timeout`	
	Reassembly timeout
`redirect`	Neighbor redirect
`renum-command`	Router renumbering command
`renum-result`	Router renumbering result
`renum-seq-number`	
	Router renumbering sequence number reset
`router-advertisement`	
	Neighbor discovery router advertisements
`router-renumbering`	
	All router renumbering
`router-solicitation`	
	Neighbor discovery router solicitations
`time-exceeded`	All time exceeded messages
`unreachable`	All unreachable
`<0-255>`	ICMPv6 message type
`<0-255>`	ICMPv6 message code
`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.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected

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 fragments
```

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.

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 the sequence numbers of an IPv6 access list specification.

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.

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, VLAN identifier, inner VLAN identifier, flow label, and fragment 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) (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>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
  af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|)
  ((flow-label <0-1048575>)|)(fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)
  (log|) (sample|)((redirect-to-port IFNAME)|)
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>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23|
  af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
  ef)|) ((flow-label <0-1048575>)|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-
  4094>|)(log|) (sample|)((redirect-to-port IFNAME)|)
```

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>	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.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected

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 fragments
```

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.

Command Syntax

```
(<1-268435453>|)(deny|permit) (tcp) (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>|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>)| (fragments) |} (((dscp (<0-63>| af11| af12| af13| af21| af22|
  af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
  default| ef ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|)

(<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 ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

(<1-268435453>|)(deny|permit) (udp) (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>|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>) | (fragments) |}
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-
  1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-
  to-port IFNAME)|)

(<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 ))|) (flow-label <0-1048575>|)
  (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port
  IFNAME)|)

no (<1-268435453>|)(deny|permit) (tcp) (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>|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>)|
  (fragments) |} (((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|)
  (flow-label <0-1048575>|) ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-
  4094>|) (inner-vlan <1-4094>|) (log|) (sample|)

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 ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|

no (<1-268435453>|)(deny|permit) (udp) (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>|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>) | (fragments) |} ((dscp (<0-63>| af11| af12| af13| af21| af22|
  af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
  default| ef ))|) (flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

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 ))|)
  (flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
  (sample|) ((redirect-to-port IFNAME)|)
```

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.
`host X:X::X:X`	A single source or destination host IPv6 address.
`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>`	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).
`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.
`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.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`flow-label`	IPv6 Flow-label.
`<0-1048575>`	IPv6 Flow-label value.
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected

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
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fdf2:860a:746a:e49c::/64
eq ssh
```

line vty

Use this command to move or change to ALL LINE VTY mode.

Command Syntax

```
line vty
```

Parameters

NA

Command Mode

Configure mode

Applicability

This command was introduced from OcNOS version 1.3.8

Examples

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
```

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 parameter with this command to detach a MAC access group.

Note: An access-group on egress access-group on 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 avoiding such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

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

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)#interface eth3
(config-if)#mac access-group mylist in
(config-if)#exit

(config)#interface eth3
(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 the ACL.

Command Syntax

```
mac access-list NAME
no mac access-list NAME
```

Parameters

`NAME`	Access-list name.

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 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) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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 sample
```

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, ethertype, CoS, and VLAN identifiers.

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.

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>|) (log|)
  (sample|)
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>|) (log|)
  (sample|)
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.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

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 sample
```

mac access-list remark

Use this command to add a description to an 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.

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 the 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.

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 access lists.

Command Syntax

```
show access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

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 access-list log-cache

Use this command to show the ACL logging table entries

Command Syntax

```
show access-lists log-cache
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show access-lists log-cache
2016 Oct 26 12:08:37:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto tcp, vlan 2, 0.0.0.0:0 -> 0.0.0.0:0 ...suppressed 11 times

2016 Oct 26 12:07:51:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto 255, vlan 2, 0.0.0.0 -> 0.0.0.0 ...suppressed 10 times
```

show arp access-lists

Use this command to display ARP access lists.

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 version 1.3.6.

Example

```
#show arp access-lists
ARP access list arp1
        remark "arp access-list created"
        10 permit ip any mac any
```

show ip access-lists

Use this command to display IP access list

Command Syntax

```
show ip access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

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.

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.

Command Syntax

```
show mac access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

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 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 configuration with defaults.

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#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 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

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 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

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 17 Access Control List Commands (Standard)

This chapter is a reference for the standard Access Control List (ACL) commands. Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering.

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.

A standard ACL can be used by Layer 3 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 an ACL.

Note: Standard access-lists are not allowed to be attached to 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 version 1.3.6.

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 an 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 version 1.3.6.

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.

a standard IPv6 ACL can be used by Layer 3 protocols to permit or deny IPv6 packets from a host or a range of prefixes.

Use the `no` form of this command to remove an ACL.

Note: Standard access-lists are not allowed to be attached to 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 version 1.3.6.

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 an access control entry in an access control list (ACL).This commands 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 version 1.3.6.

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
```

CHAPTER 18 Chassis Management Module Commands

This chapter provides a description, syntax, and examples of CMM feature commands:

- debug cmm
- locator led
- show hardware-information
- show system-information

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.

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 (all|fan|led|memory|power|system-
  status|temperature|transceiver)
```

Parameters

`all`	Hardware details of all modules
`fan`	Fan status of the board
`led`	LED status of the board
`memory`	Memory information of the board
`power`	Voltage, current, and power Information
`system-status`	System fault status
`temperature`	Temperature of the board
`transceiver`	Transceiver hardware details

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show hardware-information all
-------------------------------------------------------
                RAM INFORMATION
-------------------------------------------------------

Total                                   : 7885 MB
Used                                    : 475 MB (6 %)
Free                                    : 7410 MB (94 %)
Shared                                  : 9 MB
Buffers                                 : 90 MB
Total Swap                              : 0 MB
Free Swap                               : 0 MB
Current Processes                       : 209
Total High Memory                       : 0 MB
Available High Memory                   : 0 MB
Unit Size                               : 1 Bytes
Alert Threshold                         : 90 %
Critical Threshold                      : 80 %
-------------------------------------------------------
               HARD DISK INFORMATION
-------------------------------------------------------

Serial Number                           : GM201805100000000188
Model Number                            : FS032GM242I-AC
Firmware Revision                       : Q0608A  FS032GM242I-AC
Cylinders                               : 16383
```

```
Heads                                   : 16
Sectors                                 : 61865984
Unformatted Bytes/Track                 : 0
Unformatted Bytes/Sector                : 0
Revision No                             : 1008.0
Usage Alert Threshold                   : 90 %
Usage Critical Threshold                : 80 %
-------------------------------------------------------------
Filesystem   Total        Used         Free         Use%
-------------------------------------------------------------
/            28858        3445         25413        12%
/cfg         476          42           434          9%
-------------------------------------------------------------

Codes : R - Rear Fan, F - Front Fan, U - Unknown
-------------------------------------------------------------
FAN TRAY     FAN          RPM          MINRPM       MAXRPM
-------------------------------------------------------------
1            1(F)         22200        12325        23300
1            2(R)         21600        10738        20300
2            1(F)         22300        12325        23300
2            2(R)         21700        10738        20300
3            1(F)         22300        12325        23300
3            2(R)         21800        10738        20300
4            1(F)         22300        12325        23300
4            2(R)         21700        10738        20300

Board Temp Sensors Temperature in Degree C
-------------------------------------------------------------------------------
SENSOR TYPE                      CURR   EMER   ALERT  CRITI  CRITI  ALERT  EMER
                                 TEMP   MIN    MIN    MIN    MAX    MAX    MAX
-------------------------------------------------------------------------------
Temperature sensor at 0x48       25.00  1      10     14     47     65     75
Temperature sensor at 0x49       31.00  1      10     14     54     70     75
Temperature sensor at 0x4A       26.00  1      10     14     49     70     75
Temperature sensor at 0x4C       34.00  1      10     14     56     70     75
Temperature sensor at 0x4D       42.00  1      10     14     68     70     75
CPU                              27.00  1      10     14     88     98     108
FAN Board temp sensor 0x4E       23.00  1      10     14     60     70     75
FAN Board temp sensor 0x4F       23.00  1      10     14     60     70     75
BCM Chip                         58.40  1      10     14     90     100    110

BCM Chip Internal Temperature
-------------------------------------------
TEMP MONITOR    CURRENT TEMP    PEAK TEMP
                (Degree C)      (Degree C)
-------------------------------------------
1               55.50           60.80
2               57.90           61.80
3               56.40           60.80
4               55.50           60.30
5               55.90           60.80
6               58.40           62.80
7               56.90           61.80
8               58.40           63.20

-----------------------------------------------------
                System Power Information
-----------------------------------------------------
CMM_PS1_12V_PG                          : FAIL
CMM_PS2_12V_PG                          : GOOD
CMM_PS1_AC_ALERT                        : FAIL
CMM_PS2_AC_ALERT                        : GOOD

Codes:     * Not Supported by device    NA Not Applicable

PSU        VOLT-IN    VOLT-OUT   CURR-IN    CURR-OUT   PWR-IN     PWR-OUT    TEMP-1     TEMP-2     FAN-1      FAN-2
           (Volt)     (Volt)     (Ampere)   (Ampere)   (Watt)     (Watt)     (Celsius)  (Celsius)  (Rpm)      (Rpm)
Max                                                               800.00
-------------------------------------------------------------------------------------------------------------------
2          225.00*    12.02*     1.19*      21.13*     270.00*    254.00*    30.00*     34.00*     2560*      NA*

-------------------------------------------------
```

```
LED             COLOR              DESCRIPTION
-------------------------------------------------
POWER 1         SOLID AMBER        PSU1 present, No Power
POWER 2         GREEN              PSU2 operates Normally
FAN TRAY 1      GREEN              Normal
FAN TRAY 2      GREEN              Normal
FAN TRAY 3      GREEN              Normal
FAN TRAY 4      GREEN              Normal
SYSTEM          RED                Error/Fault/Failure
LOCATOR         AMBER OFF          Locator led OFF
FRONT FAN       SOLID GREEN        Fan operates normally

-----------------------------------------------------
           Transceiver DDM support list
-----------------------------------------------------
Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FCCN410QD3C
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTL410QE4C
DDM Supported               :Yes

Type                        :QSFP28
Vendor Name                 :DELL
Vendor Part Number          :4WJ41
DDM Supported               :Yes

Type                        :QSFP28
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FCBN425QE1C
DDM Supported               :Yes

Type                        :QSFP28
Vendor Name                 :FINISAR CORP.
Vendor Part Number          :FTLC1151RDPL
DDM Supported               :Yes

Type                        :QSFP28
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTLC9551REPM
DDM Supported               :Yes


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
-----------------------------------------------

QSFP:[1-16]
-------------------------------------------------------------------------------------------------
PORT   PRESENCE        RESET      POWER                                  LANE
-------------------------------------------------------------------------------------------------
                                                        1          2          3          4
-------------------------------------------------------------------------------------------------
1      Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
2      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
```

```
                                        Tx-Los     Off        Off        Off        Off
3      Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
4      Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
5      Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
6      Present         Normal     -     Tx         on         on         on         on
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
7      Present         Normal     -     Tx         on         on         on         on
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
8      Present         Normal     -     Tx         on         on         on         on
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
9      Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
10     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
11     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
12     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
13     Present         Normal     -     Tx         on         on         on         on
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
14     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
15     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
16     Not Present     Normal     -     Tx         off        off        off        off
                                        Rx-Los     Off        Off        Off        Off
                                        Tx-Los     Off        Off        Off        Off
Codes:
XCVR - Transceiver      DSP - DigitalSignalProcessor

SLOT:[1-8]
-------------------------------------------------------------------------------
Slot OpticalModule Cardtype DSPvendor|            XCVRpresence  XCVRvendor|
                            SerialNo|                           SerialNo|
                            FirmwareVersion                     FirmwareVersion
-------------------------------------------------------------------------------
1    Present       ACO      NEL                  Present       OCLARO
                            100877111/SMV029507                SMV029507
                            180d.a044/101.9                    101.9
8    Not-Present   -        -                    Not-Present   -

Maximum license available : 2  Unused license count : 0
System Over all status   : Minor Fault

---------------------------
Components status
---------- ----------------
CPU        : Normal
RAM        : Normal
DISK       : Normal
TEMP       : Normal
FAN        : Normal
POWER      : Minor Fault
SOFTWARE   : Normal

Codes: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major
```

```
Component  Fault  Timestamp            Thresh   Violation-Status
---------  -----  ---------            ------   ----------------
FAN        H-Mi   12-11-2019 10:08:03          Tray[4] Fan[2] set to MIN RPM[52.90]
                  12-11-2019 10:08:03          Tray[4] Fan[1] set to MIN RPM[52.90]
                  12-11-2019 10:08:03          Tray[3] Fan[2] set to MIN RPM[52.90]

POWER      H-Mi   12-11-2019 10:08:01          Psu [1] AC is not OK and 12V Power Failed
```

Table 18-54 explains the show command output fields.

Table 18-54: 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 in the port.

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
`fan`	Fan EEPROM Information
`psu`	PSU EEPROM Information
`os`	OS Version Information
`cpu`	Processor Information
`bios`	BIOS Information
`cpu-load`	CPU Load Information
`board-info`	Board Details

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system-information board-info

System Board Information
========================
Product Name             : 7716-24SC-O-AC-F
Part Number              : FP3ZZ7624004A
Serial Number            : 771624SC1904016
Base MAC Address         : B8:6A:97:0B:F9:B6
Manufacture Date         : 02/03/2019 15:32:20
Label Revision           : R01A
Platform Name            : x86_64-accton_as7716_24xc-r0
ONIE Version             : 2017.11.00.03
MAC Addresses            : 131
Manufacturer             : Accton
Country Code             : TW
Vendor Name              : Edgecore
Diag Version             : 0.0.0.19
CRC-32                   : 0xC0826278
```

```
Switch Chip Revision    : BCM56965_A1
Sys Cpld Board Pcb Id   : ES7624BT2(MAX-10M0DC)
Fan Board Id            : ZZ Project
CPLD 1 Version          : 5
CPLD 2 Version          : 7
CPLD 3 Version          : 7
Fan CPLD Version        : 3
USB VBUS                : Disabled
```

```
#show system-information all

System Fan FRU Information
==========================

%FAN Tray  [1] EEPROM Information is not supported

%FAN Tray  [2] EEPROM Information is not supported

%FAN Tray  [3] EEPROM Information is not supported

%FAN Tray  [4] EEPROM Information is not supported

System PSU FRU Information
==========================

%PSU [2] EEPROM Information is not available

System Board Information
========================
Product Name            : 7716-24SC-O-AC-F
Part Number             : FP3ZZ7624004A
Serial Number           : 771624SC1904016
Base MAC Address        : B8:6A:97:0B:F9:B6
Manufacture Date        : 02/03/2019 15:32:20
Label Revision          : R01A
Platform Name           : x86_64-accton_as7716_24xc-r0
ONIE Version            : 2017.11.00.03
MAC Addresses           : 131
Manufacturer            : Accton
Country Code            : TW
Vendor Name             : Edgecore
Diag Version            : 0.0.0.19
CRC-32                  : 0xC0826278
Switch Chip Revision    : BCM56965_A1
Sys Cpld Board Pcb Id   : ES7624BT2(MAX-10M0DC)
Fan Board Id            : ZZ Project
CPLD 1 Version          : 5
CPLD 2 Version          : 7
CPLD 3 Version          : 7
Fan CPLD Version        : 3
USB VBUS                : Disabled

Host System Details
===================
OS Distribution :       Debian GNU/Linux 8.2 (jessie)
Kernel Version  :       3.16.7-gcc61b01-ec-as7716-24sc


System CPU Information
======================
Processor       : 1
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 2
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 3
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 4
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 5
```

```
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 6
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 7
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz
Processor       : 8
Model           : Intel(R) Xeon(R) CPU D-1518 @ 2.20GHz

System BIOS Information
=======================
# dmidecode 2.12
SMBIOS 3.0 present.
# SMBIOS implementations newer than version 2.8 are not
# fully supported by this version of dmidecode.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
        Vendor: American Megatrends Inc.
        Version: AS7716 V31 20170906
        Release Date: 09/06/2017
        Address: 0xF0000
        Runtime Size: 64 kB
        ROM Size: 8128 kB
        Characteristics:
                PCI is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                Boot from CD is supported
                Selectable boot is supported
                BIOS ROM is socketed
                EDD is supported
                5.25"/1.2 MB floppy services are supported (int 13h)
                3.5"/720 kB floppy services are supported (int 13h)
                3.5"/2.88 MB floppy services are supported (int 13h)
                Print screen service is supported (int 5h)
                8042 keyboard services are supported (int 9h)
                Serial services are supported (int 14h)
                Printer services are supported (int 17h)
                ACPI is supported
                USB legacy is supported
                BIOS boot specification is supported
                Targeted content distribution is supported
                UEFI is supported
        BIOS Revision: 5.11

Handle 0x0052, DMI type 13, 22 bytes
BIOS Language Information
        Language Description Format: Long
        Installable Languages: 1
                en|US|iso8859-1
        Currently Installed Language: en|US|iso8859-1



System CPU-Load Information
===========================

Uptime                    : 0 Days 20 Hours 26 Minutes 51 Seconds

Load Average(1 min)       : 1.56% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.72% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 4.23% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 0.36%
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          : 0.95% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 5 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 6 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 7 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 8 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
```

The following tables explain the show command output fields.

Table 18-55: 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 18-56: 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.
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

Table 18-56: Show system BIOS information (Continued)

BIOS Information	Description
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 18-57: 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 18-58: 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.
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 18-59: Show system board information

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated

Table 18-59: (Continued)Show system board information

System Information	Description
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
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 18-60: 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.

CHAPTER 19 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 (PORTNUM|)
```

Parameters

PORTNUM	Port number. If this parameter is not specified, this command clears the transceiver alarms for all interfaces.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ddm transceiver alarm
```

ddm monitor

Use this command to enable DDM monitoring for interfaces which have a supported transceiver.

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor
no ddm monitor
```

Parameters

None

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
(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 19-61 explains the output fields.

Table 19-61: 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.

CHAPTER 20 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
```

Table 20-62 explains the output fields.

Table 20-62: show monitor fields

Entry	Description
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then: 1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory. 2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.

Table 20-62: show monitor fields

Entry	Description
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but 1. In case of local monitoring, if the destination port link state is down, then session will be in this state. 2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state. 3. In case the sources configured are ports and none of them are in link up state, then session will be in this state. 4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: 1. Destination port exceeding maximum limit. 2. Filters exceeding maximum limit. 3. VLAN source ports exceeding maximum limit. In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.

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 20-63 explains the output fields.

Table 20-63: show monitor session output fields

Entry	Description
Type	Type of monitor session.
State	State of the security flow filter. There are different error messages when you do RSPAN configuration: 1. Session admin shut 2. Dst in wrong mode 3. No sources configured 4. No dest configured 5. No operational src/dst 6. No hardware resource 7. Hardware failure.
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then: 1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory. 2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but: 1. In case of local monitoring, if the destination port link state is down, then session will be in this state. 2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state. 3. In case the sources configured are ports and none of them are in link up state, then session will be in this state. 4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: 1. Destination port exceeding maximum limit. 2. Filters exceeding maximum limit. 3. VLAN source ports exceeding maximum limit. In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.

Table 20-63: show monitor session output fields

Entry	Description
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).
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

#
```

CHAPTER 21 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 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 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 sampling 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.

Command Mode

Interface mode

Parameters

None

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 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 21-64: 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 about the output 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 about the output of this command, see the show sflow command.

```
#show sflow statistics

sFlow Port Statistics:
Interface  Packet-Sampling   Counter-Polling
                Count              Count
---------  ---------------   ---------------
xe1                      0                19
```

CHAPTER 22 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
Failover Group 1 : Enable
No. of links to trigger failover : 0
MPG Port         CPG Port
--------------------------
   xe1            xe17
No. of times MPG link failure : 0
No. of times MPG link recovered : 0
No. of times MPG link in blocking state : 0
No. of times MPG link in forwarding state : 0
No. of times CPG got auto disabled : 0
No. of times CPG got auto enable : 0
```

Table 22-65 Explains the show command output fields.

Table 22-65: 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
```

CHAPTER 23 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
```

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 23-66 explains the output:

Table 23-66: Virtual router log clients

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 23-67 explains the output:

Table 23-67: Virtual router log terminals

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 23-68 explains the output:

Table 23-68: Virtual router statistics

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 24 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 24-69.

This chapter contains these commands:

Syslog Severities

Table 24-69: 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.
		Warning messages are also logged in this level.
		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:
		`OSPF Received link up for interface: xe1`
		`OSPF neighbour [10.1.1.1] Status change Exstart -> Exchange`
		`Interface %s changed state to UP`

Table 24-69: 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

OcNOS rotates `/var/log/message` every three hours. When the log file is 100 megabytes or more, the current log file is backed up and a new log file is started. With four rotations, there can be four backup log files and one current log file.

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 24-69.

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 24-69.

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)#2015Dec2303:13:26OcNOSBGP-6:[RIB]ScanningBGPNetworkRoute
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 24-69. 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: OcNOS shell takes level of CMLD module. Any updates in severity of CMLD will be taken into effect for the next OcNOS session.

Command Syntax

```
logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|onm|oam|ospf|ospf6|pim|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow|
  trill|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|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow|
  trill|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
`pservd`	PSERVD messages
`ptp`	PTP messages
`rib`	RIB messages

`rip`	RIP messages
`ripng`	RIPNG messages
`rmon`	RMON messages
`rsvp`	RSVP messages
`sflow`	Sflow messages
`trill`	TRILL messages
`vrrp`	VRRP messages
`<0-7>`	Severity level as shown in Table 24-69.

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".

The "mylogFile" file will have the latest log information. As soon as it’s size becomes 1 MB, this file is renamed as mylogFile.0 and new log information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost to accommodate a new set of log entries in mylogFile.

Use option no to cancel writing to a specific log file.

Note: Changes to `logfile` parameters (name/size/severity) take effect at 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 24-69.
`<4096-4194304>`	Log file size in bytes.

Default

The default severity level is 6 (debug informational).

The default log file size is 419430400 bytes.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#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 24-69.

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 24-69. If not specified, the default is 7.

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 7 (debug detailed).

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 24-69. If not specified, the default is 7.
`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 7 (debug detailed).

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
```

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 OcNOS NSM-3: AgentX: failed to send open message: Connection
refused
2016 Mar 03 00:02:33 OcNOS OSPF-3: AgentX: failed to send open message: Connection
refused
2016 Mar 03 00:02:33 OcNOS OSPFv3-3: AgentX: failed to send open message: Connection
refused
2016 Mar 03 00:02:33 OcNOS IS-IS-3: AgentX: failed to send open message: Connection
refused
2016 Mar 03 00:02:33 OcNOS BGP-3: AgentX: failed to send open message: Connection
refused
2016 Mar 03 00:02:33 OcNOS 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 24-70 explains the output fields.

Table 24-70: 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 500 end-seqn 750
```

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

```
#show logging logfile start-time 2015 mar 15 12:10:00 end-time 2015 apr 15
12:10:00
```

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 25 Linux Shell Commands

This chapter is a reference for Linux shell 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 26 System Configure Mode Commands

This chapter provides a reference for system-level configure mode commands.

forwarding custom-profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use the `forwarding custom-profile default` command (with no parameters) to set the forwarding table size to its default.

Command Syntax

Tomahawk platform:

```
forwarding custom-profile {l2-banks <1-4>|l3-banks <1-4>|lpm-banks 2}
```

Helix4 platform:

```
forwarding custom-profile {l2-banks <1-24>|l3-banks <1-23>|vlan-xlate-banks <1-
  23>|ep-vlan-xlate-banks <1-23>}
```

Tomahawk and Helix4 platforms:

```
forwarding custom-profile default
```

Parameters

`l2-banks`	L2 banks. Unspecified banks are used as L2 banks.
`<1-4>`	Number of L2 banks. Each bank size is 32k entries and each entry is 105 bits.
`<1-24>`	Number of L2 banks. Each bank size is 1k entries and each entry is 420 bits.
`l3-banks`	L3 banks. Unspecified banks are used as L2 banks.
`<1-4>`	Number of L3 banks. Each bank size is 32k entries and each entry is 105 bits.
`<1-23>`	Number of L3 banks. Each bank size is 1k entries and each entry is 420 bits.
`lpm-banks`	Longest-prefix match banks. Unspecified banks are used as L2 banks.
`2`	Two LPM banks per entry. The remaining banks can be used by any.
`vlan-xlate-banks`	VLAN translate banks. Unspecified banks are used as L2 banks.
`<1-23>`	Number of VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
`ep-vlan-xlate-banks`	Egress VLAN translate banks. Unspecified banks are used as L2 banks.
`<1-23>`	Number of EP VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
`default`	Use L2 profile Three; the size of the l2 table (MAC address table) and L3 table (host table) is almost equal.

Default

By default, the forwarding table size is L2 profile three: the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command only applies to Tomahawk and Helix4 platforms.

Examples

```
#configure terminal
(config)#forwarding custom-profile l3-banks 4
```

forwarding profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Note: The use of `k` for “kilo” (as in 1k) does not equal 1,000. In all cases, `k` equals the Boolean value: 1,024.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use this `no` command to set the forwarding table size to the default.

Command Syntax

```
forwarding profile (l2-profile-one | l2-profile-two | l2-profile-three | l3-profile
  | l3-128bit-profile | lpm-profile | lpm-128bit-profile)
no forwarding profile
```

Parameters

For details about these profiles, see show forwarding profile limit.

`l2-profile-one`	L2 profile One
`l2-profile-two`	L2 profile Two
`l2-profile-three`	L2 profile Three (default); the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal
`l3-profile`	L3 profile
`l3-128bit-profile`	L3 profile with IPv6 prefix >64 support
`lpm-profile`	Longest-prefix match profile
`lpm-128bit-profile`	LPM profile with IPv6 prefix >64 support

Default

The default forwarding table size is `l2-profile-three`.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#forwarding profile l2-profile-one
```

hardware-profile filter (XGS)

Use this command to enable or disable ingress IPv4 or IPv6 and egress IPv6 filter groups. Disabling filter groups increases the configurable filter entries.

Command Syntax

```
hardware-profile filter (ingress-ipv4|ingress-ipv6|egress-ipv6|ingress-arp)
  (enable|disable)
```

Parameter

`ingress-ipv4`	IPv4 filter ingress group.
`ingress-ipv6`	IPv6 filter ingress group.
`egress-ipv6`	IPv6 filter egress group.
`enable`	Enable filter group.
`disable`	Disable filter group.
`ingress-arp`	ARP filter ingress group

Default

By default, all filter groups are enabled except the `ingress-arp` filter group.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This form of the `hardware-profile filter` command is *not* available on Qumran platforms. See hardware-profile filter (Qumran).

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
```

hardware-profile filter (Qumran)

Use this command to enable or disable ingress and egress filter groups. Disabling filter groups increases the configurable filter entries.

Command Syntax

```
hardware-profile filter (ingress-l2-group|ingress-ipv4|qos-group|egress-
  ipv4|egress-ipv6|egress-l2-group) (enable|disable)
```

Parameter

`ingress-l2-group`	Layer 2 (MAC) filter ingress group.
`ingress-ipv4`	IPv4 filter ingress group.
`qos-group`	QoS filter group.
`egress-ipv4`	IPv4 filter egress group.
`egress-ipv6`	IPv6 filter egress group.
`egress-l2-group`	Layer 2 (MAC) filter egress group.
`enable`	Enable filter group.
`disable`	Disable filter group.

Default

By default, all filter groups are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms. For other platforms, see hardware-profile filter (XGS).

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
```

hardware-profile flowcontrol (Qumran)

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 on Qumran platforms.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile flowcontrol enable
```

hardware-profile statistics (Qumran)

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.

Command Syntax

```
hardware-profile statistics (ingress-acl|mpls-ac|mpls-lsp|mpls-pwe)
  (enable|disable)
```

Parameter

`ingress-acl`	Ingress ACL statistics.
`mpls-ac`	Attachment circuit statistics.
`mpls-lsp`	LSP statistics.
`mpls-pwe`	Pseudowire logical interfaces statistics.
`enable`	Enable statistics.
`disable`	Disable statistics.

Default

By default, filter statistics are disabled.

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 statistics mpls-lsp enable
```

load-balance rtag7

Use this command to configure rtag7 load balancing.

Use the `no` option to disable the rtag7 load balancing.

Command Syntax

This form enables or disables rtag7 load balancing globally:

```
load-balance rtag7
no load-balance rtag7
```

By default, load balancing is enabled for ECMP, LAG, and TRILL.

This form sets rtag7 hashing for ECMP and L3 LAG based on IPv4 fields:

```
load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-id})
no load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-
  id})
```

By default, IPv4 ECMP is configured with the fields `src-ipv4`, `dest-ipv4`, `srcl4-port`, and `dest-l4port`.

By default, L3 LAG is configured with the fields `src-ipv4` and `dest-ipv4`.

This form sets rtag7 hashing for ECMP based on IPv6 fields:

```
load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr})
no load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr})
```

By default, IPv6 ECMP is configured with the fields `src-ipv6`, `dest-ipv6`, `srcl4-port`, and `dest-l4port`.

This form sets rtag7 hashing for L2 LAG based on L2 fields:

```
load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
no load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
```

By default, L2 LAG is configured with the fields `src-mac` and `dest-mac`.

This form sets rtag7 hashing on an MPLS egress LER node based on L2/L3 fields:

```
load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
  (inner-l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id}))))
no load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
  (inner-l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id}))))
```

Please note the following:

- For ingress LER nodes, hashing is done on L2 fields, L3 fields (outer IPx), or inner IP fields (only for IPx-over-IPx or IPx-over-GRE-IPx).
- For egress LER nodes, hashing is done based on only L2 and L3 fields immediately after the MPLS header which is popped. Any other fields are not supported.

This form sets rtag7 hashing based on TRILL fields:

```
load-balance rtag7 (trill (outer-l2|inner-l2|inner-l3))
no load-balance rtag7 (trill (outer-l2|inner-l2|inner-l3))
```

By default, TRILL is configured with the inner-l2 header's inner SMAC and DMAC.

This form sets rtag7 hashing based on the outer IP address:

```
load-balance rtag7 (tunnel outer-l3-header)
no load-balance rtag7 (tunnel outer-l3-header)
```

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
`next-hdr`	Next header field for IPv6
`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
`trill`	Load balance TRILL packets
`outer-l2`	TRILL outer l2 header (outer SMAC, outer DMAC, outer VLAN)
`inner-l2`	TRILL inner l2 header (inner SMAC, inner DMAC, inner VLAN, TRILL tunnel)
`inner-l3`	TRILL inner l3 header (inner SIP, inner DIP, L4 src/dest port)
`tunnel`	Load balance tunneled packets based on outer header (default uses the inner-header)
`outer-l3-header`	Use outer header for hashing (ip-over-ip, ipv6-over-ip, ip-over-gre-ip, ipv6-over-gre-ip, ipv6-over-ipv6, ip-over-ipv6, ip-over-gre-ipv6, ipv6-over-gre-ipv6)
`mpls-ler`	Load balance LER packets
`inner-l2`	Load balance Inner l2 header
`dest-mac`	Destination MAC address load balancing
`src-mac`	Source MAC address
`ether-type`	Ether-type based load balancing
`vlan`	VLAN tag id
`inner-l3`	Inner l3 header
`dest-ip`	Destination IP address
`src-ip`	Source IP address

`srcl4-port`

Source L4 port based load balancing

`protocol ID`

Protocol (IPv4), nxt-hdr (IPv6)

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#load-balance rtag7
(config)#load-balance rtag7 ipv4 src-ipv4
```

load-balance rtag7 hash

Use this command to set the rtag7 hash computation method.

Use the `no` parameter to set the rtag7 hash computation method to its default.

Command Syntax

```
load-balance rtag7 hash (crc16-bisync|crc16-ccitt|crc32-lo|crc32-hi)
no load-balance rtag7 hash
```

Parameters

`crc16-bisync`	16-bit CRC16 using the binary synchronous polynomial.
`crc16-ccitt`	16-bit CRC16 using the CCITT polynomial.
`crc16-hi`	16 most significant bits of computed CRC32.
`crc16-lo`	16 least significant bits of computed CRC32

Default

The default rtag7 hash computation method is 16-bit CRC16 using the binary synchronous polynomial `(crc16-bisync)`.

Command Mode

Configure mode

Default settings

```
load-balance rtag7 hash crc16-bisync
```

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 hash crc16-ccit
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 hash crc16-ccitt
!
(config)#no load-balance rtag7 hash
(config)#
```

load-balance rtag7 macro-flow

Use this command to enable rtag7 macro-flow based hashing.

When macro-flow is enabled, a hash function is chosen dynamically based on corresponding macro flow. It is useful when hash polarization is observed in the topology.

Note: In case of topology having multiple level of split paths, macro-flow improves the distribution but can still have variation in traffic distribution. It is observed that when 2 level of hashing is present in topology (LAG after ECMP split traffic to half), 6% of variation was observed.

Use the `no` parameter to disable rtag7 macro-flow based hashing.

Command Syntax

```
load-balance rtag7 macro-flow
```

```
no load-balance rtag7 macro-flow
```

Parameters

None

Default

By default, rtag7 macro-flow based hashing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 macro-flow
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 macro-flow
!
(config)#no load-balance rtag7 macro-flow
```

show forwarding profile limit

Use this command to show all the forwarding table sizes.

Note: The use of `k` for “kilo” (as in 1k) does not equal 1,000. In all cases, `k` equals 2 ^10: 1,024.

Command Syntax

```
show forwarding profile limit
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show forwarding profile limit

 Configured profile : custom-profile
 Forwarding profile : custom-profile(Active in hardware)

 ------------------------------------------------------------------------
|                     Forwarding Profile Table Size                      |
|------------------------------------------------------------------------|
|Profile Name    |MAC    |Host-Table   |Prefix-     |Vlan-   |Egress-    |
|                |ADDR   |Table(UC)    |Table(UC)   |xlate-  |Vlan-xlate |
|                |Table  |IPV4  |IPv6  |IPV4  |IPV6 |Table   |Table      |
 ------------------------------------------------------------------------
  l2-profile-one      96k     0k     0k     8k    4k       0k        0k
  l2-profile-two      64k     8k     4k     8k    4k       8k        8k
l2-profile-three      32k    16k     8k     8k    4k      16k       16k
      l3-profile       4k    92k    46k     8k    4k       0k        0k
  custom-profile     576k    60k    30k     8k    4k       0k        0k#
```

Table 26-71 explains the show command output fields.

Table 26-71: show forwarding profile limit output

Field	Description
Profile Name	Names of the forwarding profiles
MAC ADDR Table	MAC address table sizes
Host-Table (UC) IPv4	IPv4 unicast host table sizes
Host-Table (UC) IPv6	IPv6 unicast host table sizes
Prefix-Table (UC) IPv4	IPv4 unicast prefix table sizes
Prefix-Table (UC) IPv6	IPv6 unicast prefix table sizes
Vlan-xlate-Table	Number of VLAN translate banks
Egress-Vlan-xlate-Table	Number of egress VLAN translate banks

show hardware-profile filters

Use this command to check the status of hardware filter groups. Status is not shown for filter groups which are disabled.

Command Syntax

```
show hardware-profile filters
```

Parameters

None

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is *not* available on Qumran platforms.

Examples

```
#show hardware-profile filters

INGRESS:
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
QOS                  244       5     12        256     256         0
L2-ACL               253       1     3         256     256         0
IPV4-ACL             256       0     0         256     256         0
ARP-ACL              242       5     14        256     256         0

EGRESS:
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
L2-ACL/IPV4-ACL/QOS  512       0     0         512     256         256
```

Table 26-72 explains the output fields.

Table 26-72: show hardware-profile filters

Field	Description
EGRESS	Egress filtering is a process in which outbound data is monitored or restricted, usually by means of a firewall that blocks packets that fail to meet certain security requirements.
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.
Dedicated Entries	Number of TCAM filter entries dedicated to the filter group.
Shared Entries	Number of TCAM filter entries shared to the filter group.

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 | trill | 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
```

CHAPTER 27 Coherent Optics Commands

This chapter contains the coherent optics module commands.

clear error-counters

Use this command to clear the network interface and host interface error counters.

Command Syntax

```
clear coherent-module (<SLOTNUMBER> |) error-counters
```

Parameters

SLOT NUMBER	Enter the Slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.3.

Example

```
#clear coherent-module 6 error-counters
#clear coherent-module error-counters
```

coherent-module

Use this command to configure a coherent module. This command changes the mode to coherent module mode.

Command Syntax

```
coherent-module SLOT NUMBER
```

Parameters

SLOT NUMBER	Slot number of the coherent module

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#
```

debug cmm-tai

Use this command to display CMM tai debugging information.

Use the no form of this command to stop displaying CMM tai debugging information.

Command Syntax

```
debug cmm-tai
no debug cmm-tai
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#debug cmm-tai
#no debug cmm-tai
```

differential-encoding

Use this command to configure differential encoding to provide unambiguous signal reception when using some types of modulation. This comand makes the data to transmit depend not only on the current signal state, but also on the previous one.

Use the `no` form of this command to remove differential encoding.

Command Syntax

```
differential-encoding
no differential-encoding
```

Parameters

None

Default

Disabled

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#differential-encoding

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no differential-encoding
```

disable

Use this command to disable a coherent module slot.

Command Syntax

```
disable
```

Parameters

None

Default

By default, the coherent-module slot service disabled.

Command Mode

Coherent module mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#disable
```

enable

Use this command to enable a coherent module slot.

Command Syntax

```
enable
```

Parameters

None

Default

By default, the coherent-module slot service disabled.

Command Mode

Coherent module mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#enable
```

fec-type

Use this command to configure Forward Error Correction (FEC) in a host interface to obtain error control in data transmission.

Use the `no` form of this command to remove FEC.

Command Syntax

```
fec-type (fc|rs)
no fec-type
```

Parameters

`fc`	Fire code FEC
`rs`	Reed-Solomon FEC

Default

None

Command Mode

Hostif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#host-interface 0
(config-hostif)#fec-type rs

#configure terminal
(config)#coherent-module 1
(config-module)#host-interface 0
(config-hostif)#no fec-type
```

host-interface

Use this command to select a host interface in a coherent module to enter hostif mode.

Command Syntax

```
host-interface  <0-15>
```

Parameters

<0-15>	Index of a host interface in a coherent optical module.

Default

None

Command Mode

Coherent module mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#host-interface 0
```

loopback-type (hostif mode)

Use this command to send and receive data from the host interface port to verify that the port is operational.

Use the `no` form of this command to remove loopback functionality.

Command Syntax

```
loopback-type (deep|shallow)
no loopback-type
```

Parameters

`deep`	Deep line loopback
`shallow`	Shallow line loopback

Default

None

Command Mode

Hostif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#host-interface 0
(config-hostif)#loopback-type deep

#configure terminal
(config)#coherent-module 1
(config-module)#host-interface 0
(config-hostif)#no loopback-type
```

loopback-type (netif mode)

Use this command to send and receive data from the same network interface port to verify that the port is operational.

Use the `no` form of this command to remove loopback functionality.

Command Syntax

```
loopback-type (deep|shallow)
no loopback-type
```

Parameters

`deep`	Deep line loopback
`shallow`	Shallow line loopback

Default

None

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#loopback-type deep

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no loopback-type
```

losi-enable

Use this command to enable the Loss of Signal alarm on a network interface.

Use the `no` form of this command to disable the Loss of Signal alarm on a network interface.

Command Syntax

```
losi-enable
no losi-enable
```

Parameters

None

Default

Disabled

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#losi-enable

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no losi-enable
```

modulation-format

Use this command to set the modulation format of the signal.

Use the `no` form of this command to remove the configured modulation format of the signal.

Command Syntax

```
modulation-format (16-qam|32-qam|64-qam|8-qam|bpsk|dp-16-qam|dp-32-qam|dp-64-
  qam|dp-8-qam|dp-bpsk|dp-qpsk|qpsk)
```

Parameters

`16-qam`	16-quadrature amplitude modulation format
`32-qam`	32-quadrature amplitude modulation format
`64-qam`	64-quadrature amplitude modulation format
`8-qam`	8-quadrature amplitude modulation format
`bpsk`	Binary phase shift keying modulation scheme
`dp-16-qam`	Dual polarization 16-ary quadrature amplitude modulation format
`dp-32-qam`	Dual polarization 32-ary quadrature amplitude modulation format
`dp-64-qam`	Dual polarization 64-ary quadrature amplitude modulation format
`dp-8-qam`	Dual polarization 8-ary quadrature amplitude modulation format
`dp-bpsk`	Dual polarization binary phase-shift keying
`dp-qpsk`	Dual polarization quadrature phase shift keying
`qpsk`	Quadrature phase shift keying

Default

`dp-16-qam`

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#modulation-format dp-qpsk

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no modulation-format
```

network-interface

Use this command to select a network interface for a coherent module and to enter netif mode.

Command Syntax

```
network-interface <0-15>
```

Parameters

<0-15>	Index of network interface in a coherent optical module.

Default

None

Command Mode

Coherent module mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#
```

prbs-type

Use this command to set the PRBS type in a network interface to perform data integrity checks on the encapsulated packet data payloads using a pseudo-random bit stream (PRBS) pattern.

Use the `no` form of this command to remove configured PRBS type.

Command Syntax

```
prbs-type  (prbs11|prbs15|prbs20|prbs23|prbs31|prbs7|prbs9)
no prbs-type
```

Parameters

`prbs11`	Generates prbs 11 sequence
`prbs15`	Generates prbs 15 sequence
`prbs20`	Generates prbs 20 sequence
`prbs23`	Generates prbs 23 sequence
`prbs31`	Generates prbs 31 sequence
`prbs7`	Generates prbs 7 sequence
`prbs9`	Generates prbs 9 sequence

Default

None

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#prbs-type prbs31

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no prbs-type
```

pulse-shaping

Use this command to enable pulse shaping to make the transmitted signal better suited to its purpose for the communication channel, typically by limiting the effective bandwidth of the transmission.

Use the `no` form of this command to remove pulse shaping.

Command Syntax

```
pulse-shaping (rx|tx)
no pulse-shaping (rx|tx)
```

Parameters

`rx`	Enable pulse shaping for receiver
`tx`	Enable pulse shaping for transceiver

Default

By default, pulse-shaping is disabled

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#pulse-shaping tx

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no pulse-shaping tx
```

show coherent-module

Use this command to show coherent module information.

Command Syntax

```
show coherent-module SLOTNUMBER
```

Parameters

SLOTNUMBER	Slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was enhanced in OcNOS-OTN version 1.0.3.

Example

```
#show coherent-module 6
---------------------------------------------------------------
SLOT-ID : 6
---------------------------------------------------------------
Module Type                          :   DCO
Admin-Status                         :   UP
Oper-Status                          :   Initialize
Vendor-name                          :   LUMENTUM
Vendor-SN                            :   VCD19330008
Vendor-FW-Version                    :   1.5
Network-Interfaces                   :   1
Host-Interfaces                      :   2
CFP2 Vendor-name                     :   LUMENTUM
CFP2 Vendor-OUI                      :   0xF00200
CFP2 Vendor-Part                     :   TRB200DAA-01
CFP2 Vendor-SN                       :   VCD19330008
CFP2 Vendor-FW-Version               :   1.5
CFP2 Temperature                     :   43.39 °C
CFP2 Power Supply                    :   3.340 V

---------------------------------------------------------------
SLOT-ID : 6   NETIF : 0
---------------------------------------------------------------
OperStatus                           :   ready
DSP-OperStatus                       :   waiting-rx-signal
Modulation-format                    :   dp-16-qam
Differential Encoding                :   FALSE
Pulseshaping-Rx                      :
```

```
Pulseshaping-Tx                     :   FALSE
Loopback-type                       :   none
PRBS-type                           :   none
Losi-Enabled                        :
PRBS-IN-SYNC                        :   FALSE
Current PRBS BER                    :   nan
Current BER Period                  :   1000 ms
Current PRE FEC BER                 :   nan
Current POST FEC BER                :
Current Chromatic Dispersion        :   0 ps/nm
Current Differential Group Delay    :   0 ps
Tx-Disable                          :   FALSE
TX-Output-Power                     :   0.00 dBm
TX-Laser-freq                       :   193500000.000000 MHz
Min-LaserFreq                       :   191150000.000000 MHz
Max-LaserFreq                       :   196100000.000000 MHz
Current TX Laser Freq               :   193500000.000000 MHz
Grid-Spacing                        :   6.25-ghz
Laser-Grid                          :   100-ghz 50-ghz 25-ghz 12.5-ghz 6.25-ghz

Current Output Power                :   -0.08 dBm
Current Input Power                 :   -50.00 dBm
Current Post VOA Power              :
Current Prov~ Chnl Power            :   -34.50 dBm
Current Post VOA Prov~ Chnl Power   :   -34.50 dBm
Current OSNR Estimate               :   0.00 dB
Current Q-Margin                    :   0.00 dB
Current Uncorrected Block-count     :   0
Laser Age                           :   0 %

---------------------------------------------------------------
SLOT-ID : 6   HOSTIF : 0
---------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
Current PRE FEC BER                 :   nan
---------------------------------------------------------------
SLOT-ID : 6   HOSTIF : 1
---------------------------------------------------------------
Fec-type                            :   none
Loopback-type                       :   none
Current PRE FEC BER                 :   nan
```

show coherent-module faws

Use this command to show faults, alarms, and warnings (FAWS) and status of coherent module.

Command Syntax

```
show coherent-module SLOTNUMBER faws
```

Parameters

SLOTNUMBER	Slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.2.

Example

This command will only display the current FAWS of the module.

When none of the FAWS are raised.

```
#show coherent-module 6 faws
-------------------------------------------------------------------------------------
                        Fault & Status
-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
                        Alarm & Warning
-------------------------------------------------------------------------------------
```

When raised, all supported FAWS along with an event is displayed as a sample.

```
-------------------------------------------------------------------------------------
                        Fault & Status
-------------------------------------------------------------------------------------
Module General Status                       : TX-Loss-Of-Signal-Functionality
-------------------------------------------------------------------------------------
                        Alarm & Warning
-------------------------------------------------------------------------------------
 Module Alarm and Warning                        :
       Temperature                                          : Temperature Low-Warning
       Voltage-supply                                       : Power(Vcc) Low-Alarm

Network-Lane 0 Alarm & Warning              :
      Input-Power                                            : Input-Power High-Alarm
      Output-Power                                         : Output-Power Low-Alarm
      preFECBER Signal                                   : PreFECBER Signal Failure Alarm
      RX-Training-Sequence                             : [LOL]Loss-of-lock
```

```
 RX-OTU-Alarms                                    :  [LOF]Loss-Of-Frame
 RX-ODU-Alarms                                    : [BDI]Backward-Defect-Indication
 RX-OPU-Alarms                                     : [CSF]Client-Signal-Fail

  Hostif 0 PCS Alarms
Ingress-PCS-Alarms            : Loss-Of-Block-Lock
      Egress-PCS-Alarms                           : Remote-Fault
```

show coherent-module interface-mapping

Use this command to show interface mapping of coherent module.

Command Syntax

```
show coherent-module interface-mapping
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#show coherent-module interface-mapping
-------------------------------------------------
Slot-no   Module Type    Port           Hostif-no
-------------------------------------------------
1         ACO            ce17           0
                         ce18           1

2         -              ce19           -
                         ce20           -

3         -              ce21           -
                         ce22           -

4         -              ce23           -
                         ce24           -

5         -              ce25           -
                         ce26           -

6         -              ce27           -
                         ce28           -

7         -              ce29           -
                         ce30           -

8         -              ce31           -
                         ce32           -
```

show coherent-module SLOTNUMBER error-counters

Use this command to show network interface and host interface error counters of coherent module.

Command Syntax

```
show coherent-module SLOTNUMBER error-counters
```

Parameters

SLOTNUMBER	Enter slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.3.

Example

```
#show coherent-module 6 error-counters

Network-Lane 0 Counters
FEC Uncorrected Block Count          : 0
OTN Section BIP-8 Error Count        : 0

Host 0 Counters
FEC Uncorrected Block Count          : 0

Host 1 Counters
FEC Uncorrected Block Count          : 0
```

show coherent-module SLOTNUMBER interface-mapping

Use this command to show interface mapping of particular slot coherent module.

Command Syntax

```
show coherent-module SLOTNUMBER interface-mapping
```

Parameters

SLOTNUMBER	Enter slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#show coherent-module 1 interface-mapping
-------------------------------------------------
Slot-no   Module Type    Port           Hostif-no
-------------------------------------------------
1         ACO            ce17           0
                         ce18           1
```

show coherent-module monitoring-thresholds

Use this command to show alarms and warning thresholds of the coherent module.

Command Syntax

```
show coherent-module SLOTNUMBER monitoring-thresholds
```

Parameters

SLOTNUMBER	Slot number of the coherent module

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.2.

Example

```
#show coherent-module 6 monitoring-thresholds
---------------------------------------------------------------
Temperature [42.06 °C] : Monitoring Enabled
---------------------------------------------------------------
Temperature HIGH Alarm threshold       : 80.00 °C
Temperature HIGH Warning threshold   : 75.00 °C
Temperature LOW Warning threshold    : 0.00 °C
Temperature LOW Alarm threshold        : -5.00 °C

---------------------------------------------------------------
Voltage [3.336 V] : Monitoring Enabled
---------------------------------------------------------------
Voltage HIGH Alarm threshold          : 3.000 V
Voltage HIGH Warning threshold      : 3.100 V
Voltage LOW Warning threshold       : 3.600 V
Voltage LOW Alarm threshold           : 3.500 V

---------------------------------------------------------------
Input-Power [-50.00 dBm] : Monitoring Enabled
---------------------------------------------------------------
Input-Power HIGH Alarm threshold       : 4.00 dBm
Input-Power HIGH Warning threshold   : 2.00 dBm
Input-Power LOW Warning threshold    : -15.00 dBm
Input-Power LOW Alarm threshold        : -18.01 dBm
Permissible Input-Power HIGH Alarm threshold range       : -11.00 dBm to 8.00 dBm
Permissible Input-Power HIGH Warning threshold range   : -11.10 dBm to 6.99 dBm
Permissible Input-Power LOW Warning threshold range    : -30.00 dBm to 5.99 dBm
Permissible Input-Power LOW Alarm threshold range        : -40.00 dBm to 5.00 dBm
```

```
------------------------------------------------------------------
Output-Power [-0.07 dBm] : Monitoring Enabled
------------------------------------------------------------------
Output-Power HIGH Alarm threshold       : 5.00 dBm
Output-Power HIGH Warning threshold   : 3.50 dBm
Output-Power LOW Warning threshold    : -11.00 dBm
Output-Power LOW Alarm threshold        : -12.00 dBm

------------------------------------------------------------------
Pre-FEC BER [nan] : Monitoring Enabled (User-Thresholds)
------------------------------------------------------------------
Prefec signal-failure threshold        : 4.120000e-03
Prefec signal-degrade threshold     : 1.420000e-03
Prefec signal-clear threshold          : 9.200000e-04
```

show coherent-module summary

Use this command to show summary of coherent module.

Command Syntax

```
show coherent-module summary
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0 and updated in OcNOS-OTN version 1.0.2.

Example

```
#show coherent-module summary
-----------------------------------------------
Slot License Information
-----------------------------------------------
Maximum Licenses      : 8
Available Licenses        : 7
Used Licenses             : 1 [Slots : 6]

-------------------------------------------------------------------------------------------------
-----------------------------------------------
Slot ModuleStatus  FAWS   NetifOperStatus  Modulation  InputPower  preFECBER
LaserFreq

-------------------------------------------------------------------------------------------------
-----------------------------------------------
6     Ready            CLEAR   ready             dp-16-qam   -15.25dBm   8.487545e-04
193.500000THz
```

show hardware-information transceiver

Use this command to show hardware information of the transceiver.

Command Syntax

```
show hardware-information transceiver
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#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
-----------------------------------------------

QSFP:[1-16]
-------------------------------------------------------------------------------------------------
PORT   PRESENCE        RESET      POWER                                LANE
-------------------------------------------------------------------------------------------------
                                                          1          2          3          4
-------------------------------------------------------------------------------------------------
1      Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
2      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
3      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
4      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
5      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
6      Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
7      Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
```

```
8      Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
9      Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
10     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
11     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
12     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
13     Present         Normal     -          Tx         on         on         on         on
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
14     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
15     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
16     Not Present     Normal     -          Tx         off        off        off        off
                                             Rx-Los     Off        Off        Off        Off
                                             Tx-Los     Off        Off        Off        Off
Codes:
XCVR - Transceiver      DSP - DigitalSignalProcessor

SLOT:[1-8]
--------------------------------------------------------------------------------
Slot OpticalModule Cardtype DSPvendor|            XCVRpresence  XCVRvendor|
                            SerialNo|                           SerialNo|
                            FirmwareVersion                     FirmwareVersion
--------------------------------------------------------------------------------
1    Present       ACO      NEL                   Present       OCLARO
                            100877111/SMV029507                 SMV029507
                            180d.a044/101.9                     101.9
8    Not-Present   -        -                     Not-Present   -

Maximum license available : 2  Unused license count : 0
```

shutdown

Use this command to shut down a coherent module.

Use the `no` form of this command to bring up a coherent module.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

None

Command Mode

Coherent module mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#shutdown

#configure terminal
(config)#coherent-module
(config-module)#no shutdown
```

soft-tx-disable

Use this command to disable transmission of data on a network interface.

Use the `no` form of this command to enable transmission of data on a network interface.

Command Syntax

```
soft-tx-disable
no soft-tx-disable
```

Parameters

None

Default

Disabled

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#soft-tx-disable

#configure terminal
config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no soft-tx-disable
```

threshold

Use this command to set threshold values for rx-power high/low alarms and high/low warnings for network interface and to set threshold values for pre-fec-ber signal degrade/failure/clear for network interface.

Use the `no` form of this command to remove threshold values of rx-power and pre-fec-ber.

Command Syntax

```
threshold ((rx-power high-alarm VALUE1 high-warning VALUE2 low-warning VALUE3 low-alarm VALUE4) | (pre-fec-ber signal-failure VALUE5 signal-degrade VALUE6 clear VALUE7))
no threshold (rx-power | pre-fec-ber)
```

Parameters

The parameters for rx-power are high and low threshold values of alarm and warnings. For pre-fec-ber signal-failure, signal-degrade, clear threshold values

Default

None

Command Mode

Netif Mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.2.

Example

```
(config)#coherent-module 6
(config-module)#network-interface 0
(config-netif)#threshold rx-power high-alarm 4 high-warning 2 low-warning -15 low-alarm -18

(config)# coherent-module 6
(config-module )#network-interface 0
(config-netif)#threshold pre-fec-ber signal-failure 4.12e-03 signal-degrade 1.42e-03 clear 9.20e-04
```

tx-laser-freq

Use this command to set the laser frequency for a network interface in Hz, THz, GHz and MHz.

Use the `no` form of this command to remove the configured laser frequency of the network interface.

Command Syntax

```
tx-laser-freq FREQUENCY
```

Parameters

`FREQUENCY`	Enter Laser frequency in Hz|MHz|GHz|THz in the range: 191300000000000Hz-196102997874080Hz

Default

193500000.000000 MHz

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#tx-laser-freq 196102997874080Hz

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no tx-laser-freq
```

tx-output-power

Use this command to set output power of the network interface in dBm.

Use the `no` form of this command to remove configured output power of the network interface.

Command Syntax

```
tx-output-power POWER
no tx-output-power
```

Parameters

`POWER`	Transmit output power in dBm

Default

0.00 dBm

Command Mode

Netif mode

Applicability

This command was introduced in OcNOS-OTN version 1.0.0.

Example

```
#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#tx-output-power 1

#configure terminal
(config)#coherent-module 1
(config-module)#network-interface 0
(config-netif)#no tx-output-power
```

SECTION 3

Installing, Licensing, and Upgrading

Install, License, and Upgrade Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 Install, License, and Upgrade Configuration

The *OcNOS Installation Guide* contains the procedures for installing and licensing OcNOS, including:

- Downloading the OcNOS installation image.
- Downloading an OcNOS license.
- Installing OcNOS:
  - From an FTP, HTTP, or TFTP server
  - From a USB stick
  - Using Zero Touch Provisioning
- Setting up a license

OcNOS supports both patch upgrades and full upgrades:

- A patch upgrade means upgrading to a new OcNOS image with bug fixes, but without kernel changes.
- A full upgrade means upgrading to a new OcNOS ONIE image with bug fixes along with kernel changes.

The *OcNOS Installation Guide* also contains the procedures for upgrading an existing installation of OcNOS either by:

- Installing a new OcNOS version over an existing OcNOS version, which saves the existing configuration files.
- Installing a fresh version of OcNOS, which is destructive and removes existing configuration files, SSH keys, and trial licenses. You must manually restore such items from backups as needed.

Install, License, and Upgrade Command Reference

Contents

This document contains these chapters:

CHAPTER 1 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:
	`http://your-server-ip/path/to/file/IPI_deviceId.bin`
	`ftp://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
OcNOS>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.

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: 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 write command is not allowed.

Note: The URL must be compliant with RFC 3986.

Note: 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.

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

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
```

SECTION 4 # Layer 2

Layer 2 Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 VLAN Configuration

This chapter contains a complete VLAN configuration.

Configuring VLAN Tags

Topology

This shows configuring a spanning tree bridge with VLAN tags on forwarding frames. VLAN port access is configured on port `eth2` on bridge 2, port `eth2` and `eth4` on bridge 1 and port `eth4` on bridge 4. Incoming tagged packets to bridge 2 will be forwarded only on these ports configured with VLAN port access.

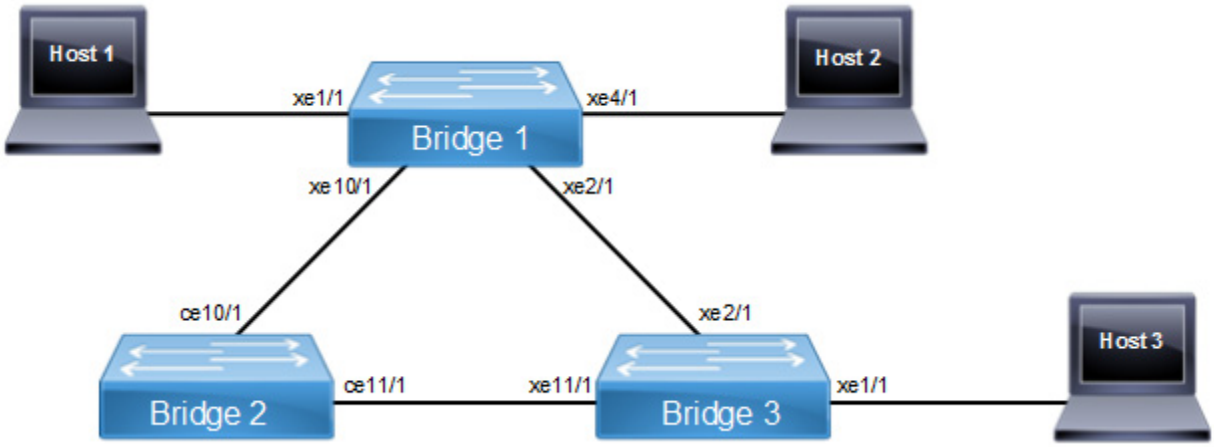


Figure 1-33: VLAN Topology

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 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`	
`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 access vlan 5`	Enable VLAN port access by specifying the VLAN ID 5 on this interface.

`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`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)


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#
```

CHAPTER 2 Spanning Tree Protocol Configuration

This chapter contains a complete sample STP configuration. STP prevents duplication of packets by eliminating loops in the network.

Topology

The following example is a simple multi-bridge topology.

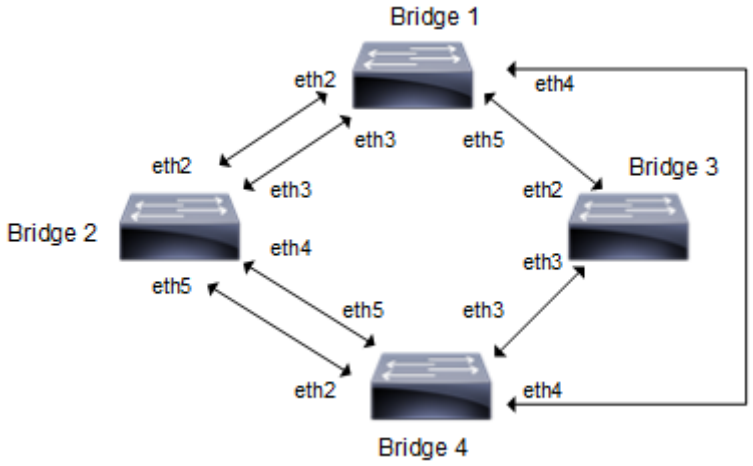


Figure 2-34: STP Topology

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)#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)#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)#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)#bridge-group 1`	Associate the interface with bridge group `1`.

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)#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)#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)#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)#bridge-group 2`	Associate the interface with bridge group `2`.

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)#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)#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)#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)#bridge-group 4`	Associate the interface with bridge group `4`.

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)#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)#bridge-group 3`	Associate the interface with bridge group `3`.

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
```

```
%   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
```

```
%   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
```

```
%   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
%
```

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 80005254000835af
%   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
%
```

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
```

```
%   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 3 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.

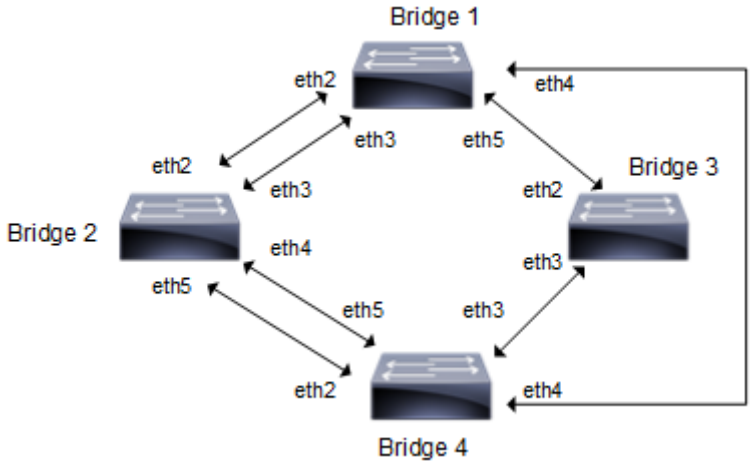


Figure 3-35: RSTP Topology

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)#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)#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)#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)#bridge-group 1`	Associate the interface with bridge group `1`.

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)#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)#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)#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)#bridge-group 2`	Associate the interface with bridge group `2`.

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)#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)#bridge-group 3`	Associate the interface with bridge group `3`.

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)#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)#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)#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)#bridge-group 4`	Associate the interface with bridge group `4`.

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
```

```
%   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
```

```
%   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
%   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
%
#
```

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 80005254000835af
%   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
```

```
%
#
```

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
%   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 4 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.

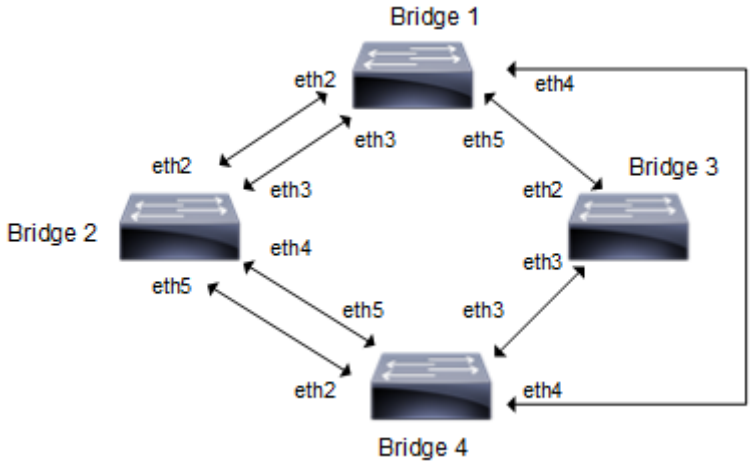


Figure 4-36: MSTP Topology

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`	same as mention above.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	same as mention above.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode for eth2
`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)#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)#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)#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`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	same as mention above.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode for eth2
`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)#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)#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)#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`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	same as mention above.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode for eth2
`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)#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`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	same as mention above.
`Bridge4(config-mst)#exit`	Exit MST Configuration mode.
`Bridge4(config)#interface eth2`	Enter interface mode for eth2
`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)#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)#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)#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 3 -  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 1000525400d15789
% 1: CIST Reg Root Id 1000525400d15789
% 1: CIST Bridge Id 8000525400244323
% 1: 26 topology change(s)  - last topology change Mon Mar  4 12:58:35 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 Rootport - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth1: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth1: Designated Port Id 0x8003 - CIST Priority 128  -
%   eth1: CIST Root 1000525400d15789
%   eth1: Regional Root 1000525400d15789
%   eth1: Designated Bridge 1000525400d15789
%   eth1: Message Age 0 - Max Age 20
%   eth1: CIST Hello Time 2 - Forward Delay 15
%   eth1: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth1: forward-transitions 1
%   eth1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   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 External Path Cost 0 -Internal Path Cost 20000
%   eth2: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400d15789
%   eth2: Regional Root 1000525400d15789
%   eth2: Designated Bridge 1000525400d15789
%   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 1 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Version Multiple Spanning Tree Protocol - Received 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 Designated - State
Forwarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth3: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400d15789
%   eth3: Regional Root 1000525400d15789
%   eth3: Designated Bridge 8000525400244323
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Version Multiple Spanning Tree Protocol - Received None - 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 Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth4: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400d15789
%   eth4: Regional Root 1000525400d15789
%   eth4: Designated Bridge 8000525400244323
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received None - 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
%

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002525400244323
% 1: MSTI Bridge Id 8002525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8002525400244323
%   eth1: Designated Bridge 8002525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8002525400244323
%   eth2: Designated Bridge 8002525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

```
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8002525400244323
%   eth3: Designated Bridge 8002525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8002525400244323
%   eth4: Designated Bridge 8002525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003525400244323
% 1: MSTI Bridge Id 8003525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8003525400244323
%   eth1: Designated Bridge 8003525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8003525400244323
%   eth2: Designated Bridge 8003525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
```



```
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8003525400244323
%   eth3: Designated Bridge 8003525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8003525400244323
%   eth4: Designated Bridge 8003525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  4:  Vlans: 4

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8004525400244323
% 1: MSTI Bridge Id 8004525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8004525400244323
%   eth1: Designated Bridge 8004525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8004525400244323
%   eth2: Designated Bridge 8004525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8004525400244323
```

```
%   eth3: Designated Bridge 8004525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8004525400244323
%   eth4: Designated Bridge 8004525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  5:  Vlans: 5

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8005525400244323
% 1: MSTI Bridge Id 8005525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8005525400244323
%   eth1: Designated Bridge 8005525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8005525400244323
%   eth2: Designated Bridge 8005525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8005525400244323
%   eth3: Designated Bridge 8005525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
```

```
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8005525400244323
%   eth4: Designated Bridge 8005525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 3 -  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 1000525400d15789
% 1: CIST Reg Root Id 1000525400d15789
% 1: CIST Bridge Id 8000525400244323
% 1: 26 topology change(s)  - last topology change Mon Mar  4 12:58:35 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 Rootport - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth1: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth1: Designated Port Id 0x8003 - CIST Priority 128  -
%   eth1: CIST Root 1000525400d15789
%   eth1: Regional Root 1000525400d15789
%   eth1: Designated Bridge 1000525400d15789
%   eth1: Message Age 0 - Max Age 20
%   eth1: CIST Hello Time 2 - Forward Delay 15
%   eth1: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   eth1: forward-transitions 1
%   eth1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   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 External Path Cost 0 -Internal Path Cost 20000
%   eth2: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400d15789
%   eth2: Regional Root 1000525400d15789
%   eth2: Designated Bridge 1000525400d15789
```

```
%   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 2
%   eth2: Version Multiple Spanning Tree Protocol - Received 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 Designated - State
Forwarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth3: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400d15789
%   eth3: Regional Root 1000525400d15789
%   eth3: Designated Bridge 8000525400244323
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Version Multiple Spanning Tree Protocol - Received None - 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 Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth4: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400d15789
%   eth4: Regional Root 1000525400d15789
%   eth4: Designated Bridge 8000525400244323
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received None - 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%
#
```

CHAPTER 5 Disable Spanning Tree Configuration

This chapter describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Topology

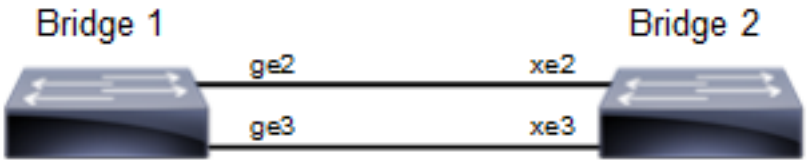


Figure 5-37: Disable Spanning Tree Topology

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 6 RPVST+ Configuration

This chapter contains a complete example of an RPVST+ configuration.

Topology

Figure 6-38: RPVST+ configuration

Configuration

Switch 2

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an RPVST+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1,.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN 3.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#switchport`	Configure `eth2` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface/
`(config-if)#switchport mode trunk`	Configure port as trunk
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#exit`	Exit interface mode.

Switch 1

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#exit`	Exit interface mode.

Switch 3

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#exit`	Exit interface mode.

Validation

Switch2

```
#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b7bfa7
% 1: Bridge Id 8002525400b7bfa7
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
```

```
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   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
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   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
%

#show spanning-tree rpvst+ 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 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 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 External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 2 - 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
%
%
%   Instance        VLAN
%   0:              1
%   1:              2
%   2:              3



#show spanning-tree rpvst+ detail
% 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 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 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 External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   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 External Path Cost 0 -Internal Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth2: Designated Port Id 0x8004 - Priority 128  -
```

```
%   eth2: Root 8001525400b7bfa7
%   eth2: Designated Bridge 8001525400b7bfa7
%   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
%   eth2: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   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


% Instance  1:  Vlans: 2
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   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


% Instance  2:  Vlans: 3
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
```

```
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8003525400b7bfa7
%   eth1: Designated Bridge 8003525400b7bfa7
%   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


% Instance  2:  Vlans: 3
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8003525400b7bfa7
%   eth2: Designated Bridge 8003525400b7bfa7
%   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
```

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 7-39, 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 7-39: 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
```

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

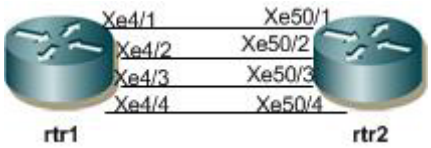


Figure 7-40: LAG Minimum Link

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
 load-interval 30
 mtu 1600
 ip address 14.4.1.2/24
 port-channel load-balance rtag7
 port-channel min-links 4
 ip ospf network point-to-point
 ip ospf cost 1000
!

#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
 load-interval 30
 mtu 1600
 ip address 14.4.1.1/24
 port-channel load-balance rtag7
 port-channel min-links 4
 ip ospf network point-to-point
 ip ospf cost 100
!

#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).

```
#show interface  po10
Interface po10
  Hardware is AGG  Current HW addr: 8cea.1b94.9194
  Physical:(Not Applicable)  Logical:(not set)
  Port Mode is Router
  Interface index: 100031
  Metric 1 mtu 1600 duplex-full
  <UP,BROADCAST,MULTICAST>
  Protocol Down (Min-Links) : True
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Jan 09 20:06:34 (00:00:10 ago)
  Statistics last cleared: 2001 Jan 02 00:32:58 (01w0d19h ago)
  inet6 fe80::8eea:1bff:fe94:9194/64
  30 second input rate 647064 bits/sec, 934 packets/sec
  30 second output rate 779117 bits/sec, 1090 packets/sec
  RX
    unicast packets 34086786 multicast packets 869896275 broadcast packets 5
    input packets 904057856 bytes 65535793854
    jumbo packets 184795
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 29
    input with dribble 0 input discard 428
    Rx pause 0
  TX
    unicast packets 52191163 multicast packets 869895836 broadcast packets 2
    output packets 922087001 bytes 83508605893
    jumbo packets 75650
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 90
    Tx pause 0

#show etherchannel

% Lacp Aggregator: po10
% Min-links : 4
% Protocol Down (Min-Links) : True
% Member:
   xe50/1
   xe50/2
```



```
   xe50/3
   xe50/4
-----------------------------------
Show interface brief | in po10

Po10          AGG    --    routed            down      PD(Min Links)   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

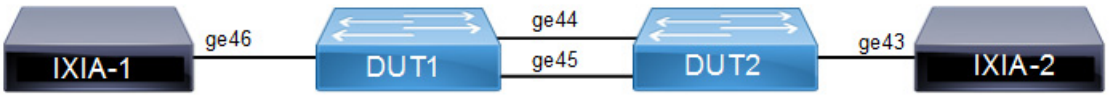


Figure 7-41: LACP force-up with Dynamic LAG

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
```

LACP force-up with McLAG

Topology

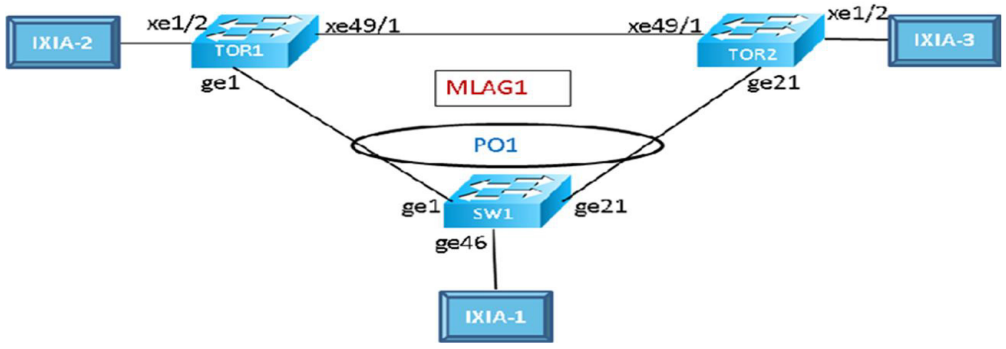


Figure 7-42: LACP force-up with McLAG

TOR1

(config)#bridge 1 protocol provider-rstp edge	Create provider rstp bridge.
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-10 type customer bridge 1 state enable	Enabling customer vlan for bridge
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service vlan for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2 svlan 2	Mapping cvlan to svlan
(config-cvlan-registration)#cvlan 10 svlan 2	Mapping cvlan to svlan
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
(config-if)#interface mlag1	Entering mlag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan 2
(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 mlag interface
(config-if)#interface po1	Entering dynamic lag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#mlag 1	Enabling mlag group number
(config-if)#interface ge1	Entering interface mode
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config-if)#channel-group 1 mode active	Add this interface to channel group 1
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between mlag domain

TOR2

(config)#bridge 1 protocol provider-rstp edge	Create provider rstp bridge.
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-10 type customer bridge 1 state enable	Enabling customer vlan for bridge
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service vlan for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2 svlan 2	Mapping cvlan to svlan
(config-cvlan-registration)#cvlan 10 svlan 2	Mapping cvlan to svlan
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
(config-if)#interface mlag1	Entering mlag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan 2
(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 mlag interface
(config-if)#interface po1	Entering dynamic lag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#mlag 1	Enabling mlag group number
(config-if)#interface ge21	Entering interface mode
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config-if)#channel-group 1 mode active	Add this interface to channel group 1
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between mlag domain

SW1

(config)#config t	Enter configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 4000-4040 bridge 1 state enable	Configure customer vlan.
(config)#interface po1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disabling spanning-tree
(config-if)#switchport mode access	Configure switchport mode as access
(config-if)#switchport access vlan 4001	Configure access vlan 4001
(config-if)#interface ge1	Entering interface mode
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 .
(config-if)#interface ge21	Entering interface mode
(config-if)#channel-group 1 mode active	Add this interface to channel group 1.
(config-if)#interface ge46	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface to hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface to hybrid and allow vlan all

Validation

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 1

TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ge21 (5046) sync: 1

SW1#show etherchannel summary
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 0002 - Oper Key 0002
     Link: ge2 (5001) sync: 1
     Link: ge22 (5021) sync: 1
```

```
TOR1#show mlag domain summary
-------------------------------------
Domain Configuration
-------------------------------------
Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-------------------------------------
MLAG Configuration
-------------------------------------
MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth              : 2g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active


TOR2#show mlag domain summary
-------------------------------------
Domain Configuration
-------------------------------------
Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-------------------------------------
MLAG Configuration
-------------------------------------
MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth              : 2g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active


TOR1#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 1001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 1001
TOR1#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 500
```

```
TOR1#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 501


TOR2#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 1001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 1001


TOR2#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 501
TOR2#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 500
```

Note: For MLAG case, admin should configure 'force-up' port either on master node or slave node only.

Example: In a static trunk environment, Preboot eXecution Environment (PXE) images are too small for most operating systems to leverage LACP during the boot process. As a result, during a PXE build process, traffic sent by the server is dropped, and the build process can fail.

To correct this situation, a port on an ICX 7750 device connected to a server that is configured as an MCT client can be set to a “force-up” state so that even if the LACPDU is not received from the server, the connected port is up and forwards packets.

To simulate this scenario we can remove channel-group configurations from the server side switch SW1 and check LACP force-up is getting enabled on TOR1:

`DUT1(config)#interface ge1`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`DUT1(config)#interface ge21`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.

DUT2

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 0 (force-up)

TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ge21 (5046) sync: 0
```



```
TOR1#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 1g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active


TOR2#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 1g
  Mlag Sync                     : IN_SYNC
  Mode                          : Standby
```

To forward traffic from ge1 of SW2:

`DUT1(config)#interface ge1`	Enter interface mode.
`DUT1(config-if)#switchport`	Make the interface as switch port.
`DUT1(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface to bridge.
`DUT1(config-if)#switchport mode access`	Configure the mode as access.

DUT1(config-if)#switchport access vlan 4001	Configure allowed vlan 4001 for the access mode.
DUT1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds.

```
TOR1#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 999
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 999
TOR1#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 999
TOR1#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0


TOR2#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 0


TOR2#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0
TOR2#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0


TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 0 (force-up)


TOR1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 14:02:ec:1c:31:5b
  Admin Key: 32769 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge1 (5026) sync: 0 (force-up)
```

```
  Collector max delay: 5


SW1#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ge1                 0.00          0            726.53        1418994
 ge46                772.68        1420362      0.00          0


TOR1#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ge1                 729.42        1424656      0.00          0
 mlag1               729.42        1424655      0.00          0
 po1                 729.43        1424658      0.00          0
```

CHAPTER 8 802.1X 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.

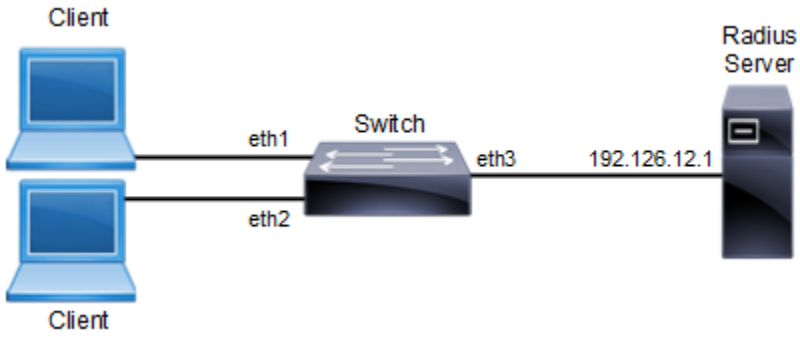


Figure 8-43: 802.1x Topology

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 192.126.12.2/24`	Set the IP address on interface `eth3`.

Validation

```
#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.168.1.1:60000
  Next radius message id: 147
```

```
  RADIUS client address: not configured


802.1X info for interface eth1
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 29
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - 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

802.1X info for interface eth2
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 29
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - 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: 192.168.1.1:60000
  Next radius message id: 147
  RADIUS client address: not configured
```

CHAPTER 9 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 9-44 displays a sample LLDP topology.

Figure 9-44: LLDP Topology

LLDPv2 (Interface Mode TLV)

Default Agent

All configuration commands in the table below should be followed for each machines.

`#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-select basic-mgmt port-description`	Enable the `port-description TLV` to be transmitted on the port

`(if-lldp-agent)# lldp tlv-select basic-mgmt system-name`	Enable the `system-name TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-capabilities`	Enable the `system-capabilities TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-description`	Enable the `system-description TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt management-address`	Enable the `management-address TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the `VLAN-id TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the `VLAN-NAME TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the `Port and Protocol VLAN id TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the `Protocol Identity TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the `VID Usage Digest TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the `Management VID TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific link-agg`	Enable the `Link Aggregation TLV` to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific max-mtu-size`	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 machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
lldp-agent
set lldp enable txrx
```

```
set lldp chassis-id-tlv ip-address
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
lldp tlv-select ieee-8021-org-specific port-vlanid
lldp tlv-select ieee-8021-org-specific vlan-name
lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
lldp tlv-select ieee-8021-org-specific ptcl-identity
lldp tlv-select ieee-8021-org-specific vid-digest
lldp tlv-select ieee-8021-org-specific mgmt-vid
lldp tlv-select ieee-8021-org-specific link-agg
lldp tlv-select ieee-8023-org-specific mac-phy
lldp tlv-select ieee-8023-org-specific max-mtu-size
set lldp timer msg-fast-tx 5
set lldp tx-fast-init 6
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
```

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    : 46
  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
```

Customer Bridge

All configuration commands in the table below should be followed for each machines.

`#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-select basic-mgmt port-description`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-name`	Enable the system-name TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-capabilities`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-description`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select basic-mgmt management-address`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the Management VID TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific link-agg`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific max-mtu-size`	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 machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface eth1
  lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  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
  lldp tlv-select ieee-8021-org-specific port-vlanid
  lldp tlv-select ieee-8021-org-specific vlan-name
  lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
  lldp tlv-select ieee-8021-org-specific ptcl-identity
  lldp tlv-select ieee-8021-org-specific vid-digest
  lldp tlv-select ieee-8021-org-specific mgmt-vid
  lldp tlv-select ieee-8021-org-specific link-agg
  lldp tlv-select ieee-8023-org-specific mac-phy
  lldp tlv-select ieee-8023-org-specific max-mtu-size
  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 machines.

`#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-select basic-mgmt port-description`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-name`	Enable the system-name TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-capabilities`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt system-description`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select basic-mgmt management-address`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8021-org-specific link-agg`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port

`(if-lldp-agent)# lldp tlv-select ieee-8023-org-specific max-mtu-size`	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 machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface eth1
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  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
  lldp tlv-select ieee-8021-org-specific port-vlanid
  lldp tlv-select ieee-8021-org-specific vlan-name
  lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
  lldp tlv-select ieee-8021-org-specific ptcl-identity
  lldp tlv-select ieee-8021-org-specific vid-digest
  lldp tlv-select ieee-8021-org-specific mgmt-vid
  lldp tlv-select ieee-8021-org-specific link-agg
  lldp tlv-select ieee-8023-org-specific mac-phy
  lldp tlv-select ieee-8023-org-specific max-mtu-size
  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                 : 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
```

LLDPV2 (Global Mode TLV)

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

Topology

Figure 9-45: 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 port description 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-if)#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 manage-ment-address	Enable LLDP port description 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
!


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
```

Machine 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.

Machine 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-class1|ep-class2|ep-class3}	Configure the med device type
(config-if)#exit	Exit interface mode.

Validation

1. Verify the LLDP configurations on Machine A

```
#show running-config lldp
!
```

```
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
lldp-agent
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
set lldp med-devtype net-connect
lldp-agent non-tpmr-bridge
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
lldp-agent customer-bridge
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
!
```

2. Verify the LLDP port statistics on machine 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 machine B

```
#show running-config lldp
!
```

```
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv-select med network-policy
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv-select med network-policy
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv-select med network-policy
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
!
```

4. Verify the LLDP port statistics on machine 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 10 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 10-46: Secured MACs learned dynamically

Send Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1 and since max limit is configured as 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
 VLAN   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
SW1#
```

Secured MAC Addresses Learned Statically

1. Stop the traffic from IXIA1 and do "`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
 VLAN   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 the 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
 VLAN   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#
```

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.

Port Security using MC-LAG

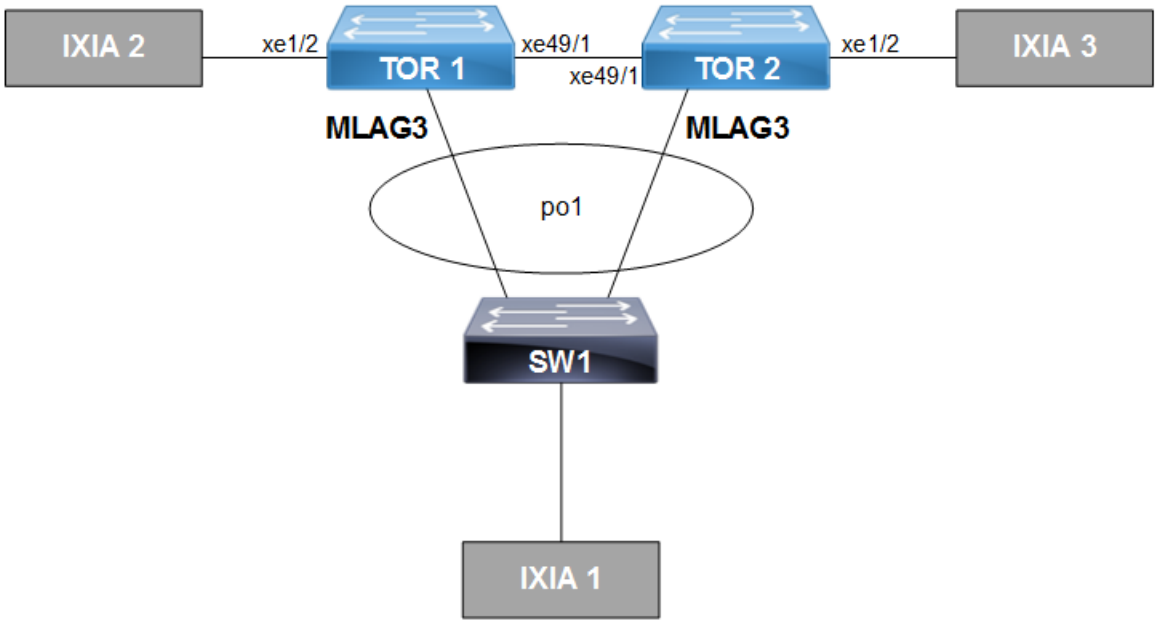


Figure 10-47: Port security with MC-LAG

TOR1

`#configgure termonal`	Enter configure mode
`(config)#bridge 1 protocol provider-rstp edge`	Create provider RSTP bridge
`(config)#vlan 2-10 type customer bridge 1 state enable`	Enabling customer vlan for bridge
`(config)#vlan 2-10 type service point-point bridge 1 state enable`	Enabling service vlan for bridge
`(config)#cvlan registration table map1 bridge 1`	Creating registration table
`(config-cvlan-registation)#cvlan 2 svlan 2`	Mapping CVLAN to SVLAN
`(config-cvlan-registation)#cvlan 10 svlan 2`	Mapping CVLAN to SVLAN
`(config-cvlan-registation)#exit`	Exit registration table mode
`(config)#interface mlag3`	Entering MLAG interface
`(config-if)#switchport`	Configuring interface as switchport
`(config-if)#exit`	Exit interface mode
`(config)#interface po1`	Entering dynamic lag interface
`(config-if)#switchport`	Configuring interface as switchport
`(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`(config-if)#switchport mode customer-edge hybrid`	Set the switching characteristics of this interface to customer edge hybrid
`(config-if)#switchport customer-edge hybrid vlan 2`	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2

(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)#mlag 3	Enabling mlag group number
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
(config-if)#exit	Enter interface mode
(config)#interface xe3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(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 vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow vlan 2
(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)#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 mlag3	Entering MLAG interface
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(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 MLAG interface
(config-if)#switchport port-security	Enabling port security
(config-if)#switchport port-security maximum 10	Limiting the maximum mac to 10
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the MLAG domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#exit	Exit MCEC mode

(config)#intra-domain-link xe49/1	Intra domain line between MLAG domain
(config-if)#domain-priority 333	Domain priority for MCEC

TOR2

(config-if)#

#configure terminal	Enter configure mode
(config)#bridge 1 protocol provider-rstp edge	Create provider RSTP bridge
(config)#vlan 2-10 type customer bridge 1 state enable	Enabling customer VLAN for bridge
(config)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service VLAN for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registation)#cvlan 2 svlan 2	Mapping CVLAN to SVLAN
(config-cvlan-registation)#cvlan 10 svlan 2	Mapping CVLAN to SVLAN
(config-cvlan-registation)#exit	Exit registration table mode
(config)#interface mlag3	Entering MLAG interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#exit	Exit interface mode
(config)#interface po1	Entering dynamic lag interface
(config-if)#Switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(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)#mlag 3	Enabling MLAG group number
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
(config-if)#exit	Exit interface mode
(config)#interface xe3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
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 vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(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)#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 mlag3	Entering MLAG interface
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(config-if)#switchport customer-edge hybrid allowed vlanall	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 MLAG interface
(config-if)#exit	Exit interface mode
mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the MLAG domain
(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between MLAG domain
(config-mcec-domain)#domain-priority 333	Domain priority for MCEC

SW1

configure terminal	Enter configuration mode
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the RSTP vlan bridge
(config)#interface po1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan
(config-if)#exit	Exit interface mode
(config)#interface xe1/3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan

(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 xe1/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan
(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 xe3/3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN

Validation

```
TOR1#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                2             mlag3        0000.0500.0200    1     54
 1                2             mlag3        0000.0500.0201    1     60
 1                2             mlag3        0000.0500.0202    1     54
 1                2             mlag3        0000.0500.0203    1     60
 1                2             mlag3        0000.0500.0204    1     54
 1                2             mlag3        0000.0500.0205    1     60
 1                2             mlag3        0000.0500.0207    1     60
 1                2             mlag3        0000.0500.0208    1     54
 1                2             mlag3        0000.0500.0209    1     60
 1                2             mlag3        0000.0500.020a    1     54
 1                2             mlag3        0000.0500.020b    1     60
 1                2             mlag3        0000.0500.020c    1     54
 1                2             mlag3        0000.0500.020d    1     60
 1                2             mlag3        0000.0500.020e    1     54
 1                2             mlag3        0000.0500.020f    1     60
 1                2             mlag3        0000.0500.0210    1     54
 1                2             mlag3        0000.0500.0211    1     60
 1                2             mlag3        0000.0500.0212    1     54
 1                2             mlag3        cc37.abbb.ed9b    1     40
```

```
TOR1#sh port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
Mlag3   dynamic             10
TOR1#
TOR1#show mac address-table count bridge 1 interface mlag3
MAC Entries for all vlans:
Dynamic Address Count: 20
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 20
TOR1#
```

Layer 2 Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Fundamental Layer 2 Commands

This chapter describes fundamental Layer 2 commands.

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.

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}
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap}
```

Parameters

`stp-bpdu-guard`	ErrDisable on stp-bpdu-guard
`lag-mismatch`	ErrDisable on lag-mismatch
`link-flap`	ErrDisable on link-flap

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 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
```

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 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 running-config switch

Use this command to display the running system switch configuration.

Command Syntax

```
show running-config switch bridge
show running-config switch dot1x
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.
`dot1x`	Display 802.1x port-based authentication 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 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 1-73: 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 1-73: 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

watch static-mac-movement

Use this command to watch if any MAC movement is detected over static MAC entries for a time period. Notification will be displaying if static MAC movement happens before the timer expires.

The counters can be validated with show interface cpu counters queue-stats for the L2 movement queue (`Tx pkts` and `Dropped pkts` columns).

Without enabling `watch static-mac-movement`, the statistics are reflected in the `Rx EGR Port Unavail` of show interface counters queue-drop-stats.

For VXLAN, `watch static-mac-movement` applies to all the MAC entries learned from the remote peer (remote dynamic or static remote), as these learned MACs are installed as static MAC entries in the hardware.

Command Syntax

```
watch static-mac-movement (<1-300>|)
```

Parameters

`<1-300>`	Timer value in seconds.

Default

By default, the timer is 10 seconds

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#watch static-mac-movement
```

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.

Command Syntax

```
bridge <1-32> acquire
no bridge <1-32> acquire
```

Parameter

`<1-32>`	Specify the 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-out time for a learned MAC address. The learned MAC address persists until this specified time.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
bridge <1-32> ageing-time <10-1000000>
bridge <1-32> ageing disable
no bridge <1-32> ageing-time
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<10-1000000>`	Specify the aging time in seconds.

Default

By default, 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>
```

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 2-74 explains the show command output fields.

Table 2-74: 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 2-75 explains the show command output fields.

Table 2-75: 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 2-75: 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) bridge <1-32> ({address MAC | interface
  IFNAME | vlan <1-4094> }|)
```

Parameter

`local`	MAC entries learned locally
`remote`	MAC entries learned from MLAG MAC sync
`<1-32>`	Bridge group
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN 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:
Total MAC Addresses in Use: 3
```

Table 2-76 explains the show command output fields.

Table 2-76: show mac address-table count output fields

Field	Description
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.

Command Syntax

```
show mac address-table (local|remote) bridge <1-32>({address MAC|interface
  FNAME|vlan <1-4094>}|)
show mac address-table count bridge <1-32>({(dynamic|multicast|static)|address
  MAC|interface IFNAME|vlan <1-4094>}|)
```

Parameter

`local`	MAC entries learned locally
`remote`	MAC entries learned from MLAG MAC sync
`<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

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table bridge 1 static interface ge14
 VLAN     MAC Address     Type      Ports
  ------+--------------+---------+---------+-------------
  1      3333.3333.3333   static    ge14

#show mac address-table bridge 1
 VLAN     MAC Address     Type      Ports
  ------+--------------+---------+---------+-------------
  1      3417.ebf6.0ace   dynamic   po1
  1      6400.6a8e.48ab   dynamic   po1
  1      a82b.b5b5.c37b   dynamic   po1
  200    0000.5e00.0101   dynamic   po1
  200    3417.ebf6.0ac5   dynamic   po1
  200    3417.ebf6.0ace   dynamic   po1
  200    6400.6a8e.48ab   dynamic   po1
  200    a82b.b5b5.c375   dynamic   po1
  200    a82b.b5b5.c37b   dynamic   po1
  800    0000.5e00.0102   dynamic   po1
  800    3417.ebf6.0ac5   dynamic   po1
```

```
800     3417.ebf6.0ace   dynamic   po1
800     6400.6a8e.48ab   dynamic   po1
800     a82b.b5b5.c375   dynamic   po1
800     a82b.b5b5.c37b   dynamic   po1
```

Table 2-77 explains the show command output fields.

Table 2-77: 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), Multiple Spanning Tree Protocol (MSTP), and Provider RSTP 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 globally on a bridge.

Use the `no` form of this command to disable MSTP globally on a bridge.

Command Syntax

```
bridge <1-32> multiple-spanning-tree enable
no bridge <1-32> multiple-spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge-group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

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 provider-rstp

Use this command to enable Provider Rapid Spanning Tree Protocol (Provider RSTP) globally on a bridge.

Use the `no` form of this command to disable Provider RSTP globally on a bridge.

Command Syntax

```
bridge <1-32> provider-rstp enable
no bridge <1-32> provider-rstp enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 provider-rstp enable

#configure terminal
(config)#no bridge 1 provider-rstp enable bridge-block
```

bridge rapid-spanning-tree

Use this command to enable Rapid Spanning Tree Protocol (RSTP) globally on a bridge.

Use the `no` form of the command to disable RSTP globally on a bridge.

Command Syntax

```
bridge <1-32> rapid-spanning-tree enable
no bridge <1-32> rapid-spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

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 Spanning Tree Protocol (STP) globally on a bridge.

Use the `no` form of this command to disable STP globally on the bridge.

Command Syntax

```
bridge <1-32> spanning-tree enable
no bridge <1-32> spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

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
bridge <1-32> spanning-tree errdisable-timeout interval <10-1000000>
no bridge <1-32> spanning-tree errdisable-timeout enable
no bridge <1-32> spanning-tree errdisable-timeout interval
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enable the timeout mechanism for the port to be enabled back
`interval`	Specify the interval after which port shall be enabled.
`<10-1000000>`	Specify the error-disable-timeout interval in seconds.

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

#configure terminal
(config)#bridge 4 spanning-tree errdisable-timeout interval 34
```

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. Refer to 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 t`e-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

Use this command to enable or disable spanning-tree on an interface.

Command Syntax

```
bridge-group <1-32> spanning-tree (disable|enable)
```

Parameters

`<1-32>`	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 3-78 Explains the show command output fields.

Table 3-78: 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.

Field	Description
Designated Path Cost	Designated cost for the interface.
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 3-79 Explains the show command output fields.

Table 3-79: 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 3-80 Explains the show command output fields.

Table 3-80: 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.

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
```

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.

Storm-control is a physical interface property and when configured on port-channel storm-control is applied on each physical member port and therefore the actual value is the configured value multiplied by the number of active member interfaces.

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 RPVST+ Commands

This chapter contains the commands used for Rapid Per VLAN Spanning Tree (RPVST+). RPVST+ enables a bridge to inter-operate with Cisco RPVST+ switches.

RPVST+ uses the Multiple Spanning Tree Protocol (MSTP) with a single VLAN for each Multiple Spanning Tree instance (MSTI). The MST bridges can have different spanning-tree topologies for different VLANs inside a region of similar MST bridges. MSTP, like the Rapid Spanning Tree Protocol (RSTP), provides rapid reconfiguration capabilities and supports load balancing.

This chapter includes the following commands:

bridge vlan

This command creates or deletes a mapping between an MSTI (Multiple Spanning Tree Instance) and a VLAN for RPVST+ operation. There can be only one VLAN per MST instance if the bridge is configured to run in RPVST+ mode.

The VLAN must have already been created. Spanning tree is enabled on each configured VLAN, and one instance of spanning-tree runs on each configured VLAN.

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

Command Syntax

```
bridge <1-32> vlan <2-4094>
no bridge <1-32> vlan <2-4094>
```

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.

Command Mode

RPVST+ configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#bridge 1 vlan 2
(config-rpvst+)#no bridge 1 vlan 2
```

bridge vlan priority

This command sets the priority value for the spanning-tree on the bridge. The lower the priority of the VLAN on a bridge, the better the chances of the bridge becoming a root bridge, or a designated bridge for the VLAN.

Use the `no` form of this command to set the priority to its default (32,768).

Command Syntax

```
bridge <1-32> vlan <2-4094> priority <0-61440>
no bridge <1-32> vlan <2-4094> priority
```

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.
`<0-61440>`	Bridge priority for the common instance. Set the priority in increments of 4096. A lower priority indicates greater likelihood of becoming root.

Default

By default, priority for each VLAN is 32,768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 vlan 2 priority 80
(config)#no bridge 1 vlan 10 priority
```

bridge-group vlan

Use this command to assign a Rapid Per-VLAN Spanning Tree (RPVST+) instance to a port.

RPVST+ uses port priority as a tiebreaker to determine which port should forward frames for a particular LAN, or which port should be the root port for a VLAN. A lower value implies a better priority. In the case of the same priority, the interface index serves as the tiebreaker, with a lower-numbered interface being preferred over others.

Use the `no` parameter with this command to remove an RPVST+ instance from this port.

Command Syntax

```
bridge-group <1-32> vlan <2-4094>
bridge-group <1-32> vlan <2-4094> path-cost <1-200000000>
bridge-group <1-32> vlan <2-4094> priority <0-240>
no bridge-group <1-32> vlan <2-4094>
no bridge-group <1-32> vlan <2-4094> path-cost
no bridge-group <1-32> vlan <2-4094> priority
```

Parameters

`<1-32>`	Bridge group identifier.
`<2-4094>`	VLAN identifier.
`<1-200000000>`	Cost of a path associated with the interface.
`<0-240>`	Port priority. A lower priority indicates greater likelihood of the interface becoming a root. Set the priority only in increments of 16.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 1 vlan 10

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 path-cost 1000

(config-if)#no bridge-group 1 vlan 10 path-cost

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 priority 240

(config-if)#no bridge-group 1 vlan 10 priority
```

bridge protocol rpvst+

Use this command to enable Rapid Per-VLAN Spanning Tree on a bridge.

Command Syntax

```
bridge <1-32> protocol rpvst+
```

Parameter

<1-32>	Bridge identifier.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 protocol rpvst+
```

bridge rapid-pervlan-spanning-tree

Use this command to enable Rapid Per-VLAN Spanning Tree (RPVST+) globally on a bridge.

Use the `no` form of this command to disable RPVST+ globally on a bridge.

Command Syntax

```
bridge <1-32> rapid-pervlan-spanning-tree enable
```

```
no bridge <1-32> rapid-pervlan-spanning-tree enable (bridge-blocked|bridge-
  forward|)
```

Parameters

`<1-32>`	Bridge identifier.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 rapid-pervlan-spanning-tree enable

(config)#no bridge 1 rapid-pervlan-spanning-tree enable bridge-forward
```

show spanning-tree rpvst+

Use this command to display RPVST information.

Command Syntax

```
show spanning-tree rpvst+
show spanning-tree rpvst+ config
show spanning-tree rpvst+ detail
show spanning-tree rpvst+ detail interface IFNAME
show spanning-tree rpvst+ interface IFNAME
show spanning-tree rpvst+ vlan <1-4094>
show spanning-tree rpvst+ vlan <1-4094> interface IFNAME
```

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`IFNAME`	Display interface information.
`<1-4094>`	Display VLAN information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following displays output of this command without any parameters.

```
#show spanning-tree rpvst+
% 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 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 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 External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
```

```
%   eth1: Root 8001525400b092de
%   eth1: Designated Bridge 8001525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 3 - 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
%
%
%   Instance        VLAN
%   0:              1, 4-10
%   1:              2
%   2:              3
```

The following displays output of this command with the `config` parameter.

```
#show spanning-tree rpvst+ config
%
%  RPVST Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xB41829F9030A054FB74EF7A8587FF58D
%-------------------------------------------------------

#show spanning-tree rpvst+ detail
% 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 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 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 External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b092de
```



```
%   eth1: Designated Bridge 8001525400b092de
%   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 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
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   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

#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   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
%

%
#show spanning-tree rpvst+ vlan 2 interface eth1
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
```

```
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   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
%
```

spanning-tree rpvst+ configuration

Use this command to enter RPVST+ configuration mode after creating a bridge and adding a VLAN to that bridge.

Internally, an RSTP Instance is created for each configured VLAN.

Command Syntax

```
spanning-tree rpvst+ configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#
```

spanning-tree vlan restricted-role

Use this command to restrict the role of the interface.

Use the `no` form of this command to not restrict the role of the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-role
no spanning-tree vlan <2-4094> restricted-role
```

Parameters

`<2-4094>`	VLAN identifier.

Default

The default is to not restrict the role of the interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-role
```

spanning-tree vlan restricted-tcn

Use this command to restrict propagating topology change notifications (TCNs) from the interface.

Use the `no` form of this command to not restrict propagating TCNs from the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-tcn
no spanning-tree vlan <2-4094> restricted_tcn
```

Parameters

`<2-4094>`	VLAN identifier.

Default

The default is to not restrict propagating TCNs

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-tcn
(config-if)#no spanning-tree vlan 10 restricted_tcn
```

CHAPTER 5 Link Aggregation Commands

This chapter describes the 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
 port-channel load-balance src-dst-mac
```

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
 port-channel load-balance src-dst-mac
!
```

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
```

port-channel load-balance

Use this command to configure LACP port-channel load-balancing and set port-selection criteria (PSC) for an interface.

Use the `no` option with this command to remove the load-balancing configuration and unset PSC.

Command Syntax

```
port-channel load-balance (dst-mac|src-mac|src-dst-mac|dst-ip|src-ip|src-dst-
  ip|dst-port|src-port|src-dst-port|rtag7)
no port-channel load-balance
```

Parameters

`dst-ip`	Destination IP address-based load balancing.
`dst-mac`	Destination MAC address-based load balancing.
`dst-port`	Destination TCP/UDP address-based load balancing.
`src-dst-ip`	Source and Destination IP address-based load balancing.
`src-dst-mac`	Source and Destination MAC address-based load balancing.
`src-dst-port`	Source and Destination TCP/UDP address-based load balancing.
`src-ip`	Source IP address-based load balancing.
`src-mac`	Source MAC address-based load balancing.
`src-port`	Source port address-based load balancing.
`rtag7`	Hashing based on packet type. IP - IP/Layer4 header, L2 - Layer2 header, TRILL - TRILL packet.

Default

By default, load balance is src-dst-port

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel load-balance src-dst-mac
```

port-channel min-bandwidth - dynamic LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(PO) interface. When the minimum number of bandwidth are configured for a LAG(PO), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(PO) is brought down. When the number of active links bandwidth 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 bandwidth that need to be up in the LAG interface.

Note: The minimum number of aggregated bandwidth 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 bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The port-channel min-links - dynamic LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

`<1-1000>g`	for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-bandwidth 10g
```

port-channel min-links - dynamic LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(PO) interface. When the minimum number of links are configured for a LAG(PO), if the active links for that interface become less than the configured value, then the whole LAG(PO) 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.

Note: The show debugging lacp feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

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 from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

port-channel min-bandwidth - static LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(SA) interface. When the minimum number of bandwidth are configured for a LAG(SA), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(SA) is brought down. When the number of active links bandwidth 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 bandwidth that need to be up in the LAG interface.

Note: The minimum number of aggregated bandwidth 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 bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The port-channel min-links - static LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

`<1-1000>g`	for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface sa1
(config-if)#port-channel min-bandwidth 10g
```

port-channel min-links - static LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(SA) interface. When the minimum number of links are configured for a LAG(SA), if the active links for that interface become less than the configured value, then the whole LAG(SA) 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.

Note: The port-channel min-bandwidth - static LAG min-bandwidth feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

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 from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface sa1
(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 5-81 explains the show command output fields.

Table 5-81: 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 5-81: 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 5-48.

Table 5-82 explains the show command output fields.

Table 5-82: 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 5-82: 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.

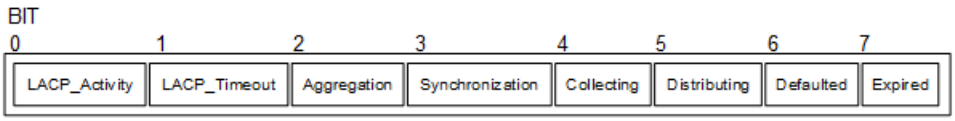


Figure 5-48: Diagram of state machine octet

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  (<1-16383>|)
```

Parameters

<1-16383>	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 1.3.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Source and Destination Mac address
-------------------------------------------
% Static Aggregator: sa3
Source and Destination Mac address
-------------------------------------------
% Static Aggregator: sa1
Source and Destination Mac address

#show static-channel 1 load-balance
% Static Aggregator: sa1
Source and Destination Mac address
```

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 <1-16383>
no static-channel-group
```

Parameter

`<1-16383>`	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
 port-channel load-balance src-dst-mac
```

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
```

```
 port-channel load-balance src-dst-mac
!
```

CHAPTER 6 VLAN and Private VLAN Commands

This chapter has the commands used to manage VLANs and private VLANs.

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 dtag vlan

Use this command to display information about VLAN double tagging.

Command Syntax

```
show dtag vlan DTAG_VLAN_ID
```

Parameters

DTAG-VLAN-IDs	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show dtag vlan 2000.3001
```

Table 6-83 explains the output.

Table 6-83: show dtag vlan output

Field	Description
Bridge	Bridge number
VLAN ID	VLAN identifier
Name	Double tag-VLAN identifers
State	VLAN state: ACTIVE, SUSPEND, or INVALID
H/W Status	Hardware status: UP or DOWN
Member ports	Interfaces that are part of the VLAN and whether untagged (u) or tagged (t)

show vlan access-map

Use this command to display information for VLAN access maps.

Command Syntax

```
show vlan access-map
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vlan access-map
Vlan access-map myMap 10
       match ip: myMap
       action: drop
```

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 6-84 Explains the show command output fields.

Table 6-84: 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 6-85 Explains the show command output fields.

Table 6-85: 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 allowed vlan dtag

Use this command to maintain a mapping between the double-tagged logical interfaces with the physical interfaces for the purpose of enabling VLAN-translation on the port alone.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Command Syntax

```
switchport trunk allowed vlan add dtag DTAG-VLAN-IDs
switchport trunk allowed vlan remove dtag DTAG-VLAN-IDs
```

Parameters

`add`	Add a mapping
`remove`	Remove a mapping
`DTAG-VLAN-IDs`	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#int mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 100,2000
(config-if)#switchport trunk allowed vlan add dtag 2000.3001
```

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 layer2 port as a host port or promiscuous 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.

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 dtag

Use this command to enable or disable double tagging packets with an outer-VLAN identifier and an inner-VLAN identifier.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Use the `no` form of this command to not double tag packets.

Command Syntax

```
vlan dtag DTAG-VLAN-IDs bridge <1-32> state (enable|disable) subscriber
no vlan dtag DTAG-VLAN-IDs bridge <1-32>
```

Parameters

`DTAG-VLAN-IDs`	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag
`<1-32>`	Bridge number
`enable`	Enable double tagging
`disable`	Suspend double tagging

Default

No default value is specified

Command Mode

VLAN database mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#vlan database
(config-vlan)#vlan dtag 2000.3001 bridge 1 state enable subscriber
```

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 7 802.1x Commands

This chapter provides a description, syntax, and examples of the 802.1X commands. It includes the following commands:

auth-mac auth-fail-action

Use this command to specify the required action after authentication fails for any source MAC (Media Access Control). If `drop-traffic` is specified, data destined to that MAC is dropped. The MAC will be added to the forwarding database in Discarded mode.

If `restrict-vlan` is specified, the unauthorized MAC is added to a restricted VLAN. The MAC will be added to the forwarding database in Forwarding mode.

Command Syntax

```
auth-mac auth-fail-action (restrict-vlan <2-4094>|drop-traffic)
```

Parameters

`drop-traffic`	Drops traffic destined to unauthorized source.
`restrict-vlan`	Adds unauthorized MAC address to restricted VLAN.
`<2-4094>`	Identity of the VLAN in the range of <2-4094>.

Default

drop-traffic

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac auth-fail-action restrict-vlan 12
```

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
auth-mac disable mode (filter|shutdown)
```

Parameters

mode	Use this parameter to disable the MAC authentication mode on an interface.
filter	Filter the frames for the MAC when in an unauthorized state.
shutdown	Shut down the interface when the MAC is unauthenticated.

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

#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable mode filter

(config)#interface eth0
(config-if)#auth-mac disable mode shutdown
```

auth-mac dynamic-vlan-creation

Use this command to enable or disable dynamic VLAN creation after successful MAC authentication.

Command Syntax

```
auth-mac dynamic-vlan-creation (enable|disable)
```

Parameters

`disable`	Disables dynamic VLAN creation: after a successful authentication, the MAC will be added to the forwarding database with the default VLAN
`enable`	Enables dynamic VLAN creation: after a successful authentication, the MAC under authentication will be added to the VLAN identifier attribute in the radius server configuration file

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation disable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation enable
```

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
auth-mac enable mode (filter|shutdown)
```

Parameters

mode	Use this parameter to enable the MAC authentication mode on an interface.
filter	Filter the frames for the MAC when in an unauthorized state.
shutdown	Shut down the interface when the MAC is unauthenticated.

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

#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable mode filter

(config)#interface eth0
(config-if)#auth-mac enable mode shutdown
```

auth-mac mac-aging

Use this command to either enable or disable MAC aging. When enabled, a MAC entry is added to the forwarding database, with aging time equal to the bridge aging time. Otherwise, the MAC entry will not be aged out. If MAC aging is disabled, the MAC entry will not be aged out.

Command Syntax

```
auth-mac mac-aging (enable|disable)
```

Parameters

`disable`	Disables MAC aging.
`enable`	Enables MAC aging.

Default

Disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging disable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging 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 initialize

Use this command to unauthorize a port, and attempt reauthentication on the specified interface.

Command Syntax

```
dot1x initialize interface IFNAME
```

Parameters

`interface`	Interface name.

Default

No default value is specified.

Command Mode

Privileged Exec

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#dot1x initialize interface eth0
```

dot1x keytxenabled

Use this command to enable or disable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant.

Command Syntax

```
dot1x keytxenabled (enable|disable)
```

Parameters

`disable`	Disables the key transmission.
`enable`	Enables the key transmission.

Default

The dot1x keytxenabled default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled disable

#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled enable
```

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 dir (in|both)
dot1x port-control (force-unauthorized|force-authorized|auto)
no dot1x port-control
```

Parameters

`auto`	Specify to enable authentication on port.
`dir`	Specify the packet control direction.
`both`	Discard receive and transmit packets from the supplicant
`in`	Discard receive packets from the supplicant
`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 HOSTNAME PORT
no ip radius source-interface
```

Parameters

`HOSTNAME`	Specify the radius client in the dotted IP address, or in the hostname format.
`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 myhost 1812

(config)#no ip radius source-interface
```

radius-server dot1x deadtime

Use this command to specify the number of minutes a radius server, which is not responding to authentication requests, is passed over by requests for radius authentication. To improve radius response times when some servers might be unavailable, use this command to cause the unavailable servers to be skipped immediately.

Use the `no` form of this command to set deadtime to the default value of 0.

Command Syntax

```
radius-server dot1x deadtime MIN
no radius-server dot1x deadtime
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`MIN`	Length of time (in minutes) that a radius server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours). Enter a value in the range 1 to 1440.

Default

Deadtime is set to 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x deadtime 10

(config)#no radius-server dot1x deadtime
```

radius-server dot1x host

Use this command to specify the IP address or host name 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|HOSTNAME|X:X::X:X)(|(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|HOSTNAME|X:X::X:X)(|(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.
`HOSTNAME`	Host name or DNS name of the RADIUS server.
`X:X::X:X`	IPv6 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 hostname auth-port 1233 timeout 1 retransmit
2

(config)#no radius-server dot1x host hostname auth-port 1233
```

radius-server dot1x key

Use this command to set the shared secret key between a Radius server and a client.

Use the `no` form of the command to undo this configuration.

Command Syntax

```
radius-server dot1x key ((0 WORD) | (7 WORD) | (WORD))
no radius-server dot1x key ((0 WORD) | (7 WORD) | (WORD))
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`0`	To specify shared key in clear-text form.
`7`	To specify shared key in encrypted form.
`WORD`	Shared secret among radius server and 802.1X client (Max Size 63).

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 dot1x key 0 abcd

#configure terminal
(config)#no radius-server dot1x 0 abcd
```

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 IEEE 802.1x port-based access control information.

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 IEEE 802.1x port-based access control information.
`diagnostics`	Display diagnostics information.
`IFNAME`	Interface name.
`sessionstatistics`	Display the statistics for a session.
`statistics`	Display the statistics.

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 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
```

The following tables describes the output of the `show dot1x` command.

Table 7-86: 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	Reauthentication period

Table 7-87: Supplicant PAE related global variables

Entry	Description
abort	Abort authentication when true
fail	Failed authentication attempt when false
start	Start authentication when true
timeout	Authentication attempt timed out when true
success	Authentication successful when true

Table 7-88: 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 7-89: Backend authentication state machine variables and constants

Entry	Description
state	State of the port.
reqCount	Number of requests sent to server
suppTimeout	Number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.
serverTimeout	Number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out.
maxReq	Maximum number of times a request packet is retransmitted to the supplicant before the authentication session times out.

Table 7-90: Controlled directions state machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)
operControlledDirections	Operational Value (Both/In)

Table 7-91: 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 7-92: 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

snmp restart auth

Use this command to restart SNMP in Authentication

Command Syntax

```
snmp restart auth
```

Parameters

None

Default

No default value is specified.

Default

The default port is UDP 162.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart auth
```

CHAPTER 8 Link Layer Discovery Protocol Commands

This chapter describes the Link Layer Discovery Protocol (LLDP) commands.

lldp debug

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

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`message`	Enable or disable NSM message debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#lldp debug event
#lldp debug messages
```

lldp ip

Use this command to set the Link Layer Discovery Protocol with an IP address to be used as a chassis and management ID.

Use the `no` form of this command to remove this value.

Command Syntax

```
lldp ip address A.B.C.D
no lldp ip address
```

Parameters

`A.B.C.D`	Enter the IP address value

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#lldp ip address 1.1.1.1
(config)#no lldp ip address
```

lldp tlv

Use this command to set the TLVs enabled for transmission on a port. Make sure that the complete set of Type Length Values (TLVs) is specified when giving this command, because TLVs not specified are disabled.

Command Syntax

```
lldp tlv {chassis-id|port-id|ttl|port-description|system-name|system-
  description|system-capabilities|management-address|ieee-8021-org-specific|ieee-
  8023-org-specific}
```

Parameters

`chassis-id`	Chassis ID type length values (TLV)
`port-id`	Port ID TLV
`ttl`	Time to live TLV
`port-description`	Port description TLV
`system-name`	System name TLV
`system-description`	System Description
`system-capabilities`	System capabilities TLV
`management-address`	Management address TLV
`ieee-8021-org-specific`	IEEE 802.1 organizationally-specific TLV
`ieee-8023-org-specific`	IEEE 802.3 organizationally-specific TLV

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lldp tlv chassis-id ieee-8021-org-specific ieee-8023-org-specific
management-address port-description port-id system-capabilities system-
description system-name ttl
```

lldp tlv-select

Use this command to configure interface LLDP parameters.

This command can be executed globally for all ports (configure mode) or locally for a specific port (interface mode).

When you give this command globally on all ports:

- The `show running-config` command only displays the options in global mode.
- A global configuration overrides an interface-level configuration. For example, if you disable an option on an interface, it is enabled after enabling the same option globally. If the option was enabled previously, the show output is suppressed and only global mode is displayed (to avoid duplicating the same configuration).
- After enabling a global configuration, when a new LLDP agent is configured on a port, it inherits the global TLV configuration. However, show output does not appear per interface/agent.
- After enabling globally, if you disable an option on an interface, the "no" form for this command is shown for that interface.
- Enabling an already enabled option causes an error.

If you disable globally on all ports:

- The option is removed globally, as well as overrides configurations for all interfaces.
- If the option was not enabled globally, it causes an error.

When enabled locally on a port:

- If the same option was enabled globally, it causes an error.
- If not already enabled, the option is enabled for the given interface alone.

When disabled locally on a port:

- If the option was not present locally or globally, it causes an error.
- If the option was enabled globally, the option is removed from this interface alone. No command will be displayed in show output.

Use the *no* form of this command to remove interface LLDP parameter configurations.

Command Syntax

```
lldp tlv-select (port-description|system-name| system-description|system-
  capabilities|management-address| ieee-8021-org-specific | ieee-8023-org-specific)
no lldp tlv-select (port-description|system-name|system-description|system-
  capabilities|management-address|ieee-8021-org-specific | ieee-8023-org-specific)
```

Parameters

`port-description`
: Port description TLV

`system-name`
: System name TLV

`system-description`
: System Description

`system-capabilities`
: System capabilities TLV

`management-address`

Management address TLV

`ieee-8021-org-specific`

IEEE 802.1 organizationally-specific TLV

`ieee-8023-org-specific`

IEEE 802.3 organizationally-specific TLV

Command Mode

Configure mode and interface mode

Example

```
#configure terminal
(config)#lldp tlv-select system-capabilities

#configure terminal
(config)#interface eth2
(config-if)#lldp-agent
(config-if-lldp-agent)#lldp tlv-select system-capabilities
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Command Syntax

```
set lldp chassis-id-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp chassis-id-tlv ip-address
```

set lldp disable

Use this command to disable the LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp disable
```

set lldp enable

Use this command to enables an LLDP agent on a port and specifies its type.

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

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp enable txrx
```

set lldp locally-assigned

Use this command to locally assign the LLDP Port ID and the Chassis ID TLV parameters.

Command Syntax

```
set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp locally-assigned port1
```

set lldp management-address-tlv

Use this command to set the management address subtype for the LLDP agent on a port.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp management-address-tlv ip-address
```

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.

Command Syntax

```
set lldp msg-tx-hold VALUE
```

Parameters

`VALUE`	Time in seconds of LLDP msg-tx-hold

Default

The default value of the `lldp msg-tx-hold` parameter is 4 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config)#set lldp msg-tx-hold 3
```

set lldp system-description

Use this command to identify the string that describes the LLDP system.

Command Syntax

```
set lldp system-description LINE
```

Parameters

LINE	Set the description of the LLDP system.

Default

The default status of Ethernet OAM is disabled.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-description LLDP agent on B1
```

set lldp system-name

Use this command to identify the system name of the LLDP function.

Command Syntax

```
set lldp system-name NAME
```

Parameters

NAME	Name of the LLDP system.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-name LLDP1
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Command Syntax

```
set lldp timer msg-tx-interval <5-32768>
set lldp timer reinitDelay VALUE
set lldp timer tx-delay <1-8192>
```

Parameters

`msg-tx-interval`	
	Set the message transmit interval value
`<5-32768>`	Set the message transmit interval value
`reinitDelay`	Set the reinit delay value
`VALUE`	Set the reinit delay value
`tx-delay`	Set the transmit delay value
`<1-8192>`	Set the transmit delay value in range of:
	(1 <= `tx-delay` <= ((0.25)* `msg-tx-interval`)

Default Values

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinitDelay` is 2 seconds.

The default value of the `tx-delay` is 2 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp timer msg-tx-interval 40

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer reinitDelay 3

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer tx-delay 3
```

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

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>
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	The limit on the number of LLDP neighbors.
`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

Interface mode

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 20 disc existing-info 1.1.1.1.1
timer 1

(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

show lldp

Use this command to display LLDP port information.

Command Syntax

```
show lldp port IFNAME
show lldp port IFNAME statistics
```

Parameters

IFNAME	The name of the interface
statistics	Display LLDP port statistics

Command Mode

Exec mode and Privileged Exec mode

Example

The following sample output from this command displays detailed information about an LLDP-enabled port.

```
#show lldp port eth0
Remote LLDP
MAC Address: 01:06:29:CF:79:A1
TTL: 60
Network Address: 192.168.1.0
Interface Name: eth1
Interface Locally Assigned String: Port-a
Interface Description: bridge
Interface Number: 2
Port Vlan ID: 1
Protocol ID: 274242030202
AutoNego Support: Supported
AutoNego Capability: 1
Operational MAU Type: 3
Link Aggregation Status: Capable
Link Aggregation Port ID: 0
Max Frame Size: 128
System name:
System Description: bridge
System Capabilities: 4
System Capabilities Enabled: 4
```

The following sample output from this command displays all LLDP statistics for a selected port.

```
#show lldp port eth0 statistics
LLDP Port statistics for eth0
Frames transmitted: 22
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Received: 5
TLVs discarded: 0
TLVs unrecognized 0
```

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

Examples

```
#snmp restart lldp
```

CHAPTER 9 Port Security Commands

This chapter describes the Port Security commands.

show port-security

Use this command to display Port Security configuration for all ports or for a particular interface.

Command Syntax

```
show port-security
show port-security (interface IFNAME |)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

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 parameter with 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 and LAG interface only. Enabling Port Security on an interface, will remove learned MAC addresses of interfaces (whether learned by static or dynamic means), and then relearn the secure MACs. Multicast MAC addresses are not considered while MAC learning limit.

Command Syntax

```
switchport port-security (static |)
no switchport port-security
```

Parameters

`static`	Static mode of Port Security.

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. Users 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 version 1.3.6.

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 enable

Use this command to enable violated MAC logging on a port security enabled interface.

Use the `no` parameter with this command to disable violated mac logging on a port security enabled interface.

Command Syntax

```
switchport port-security logging enable
no switchport port-security logging
```

Parameters

None

Default

By default logging is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

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` parameter 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>
```

Parameters

`XXXX.XXXX.XXXX`	Static secure MAC
`<2-4094>`	VLAN identifier

Default

NA

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

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 configure MAC learn limit for an interface.

Note: When a newly configured max learn limit is less than the previous value, the user must remove/flush-out the unwanted MACs to stop traffic forwarding from the unwanted Source MAC addresses. MAC addresses can be removed using "`clear mac address-table`"

Command Syntax

```
switchport port-security maximum <1-1000>
```

Parameters

`<1-1000>`	Port security maximum learn limit

Default

Default learn limit is 1.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security maximum 3
```

SECTION 5 # Layer 3

Layer 3 Unicast Configuration Guide

Contents

This guide contains these chapters:

CHAPTER 1 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.

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

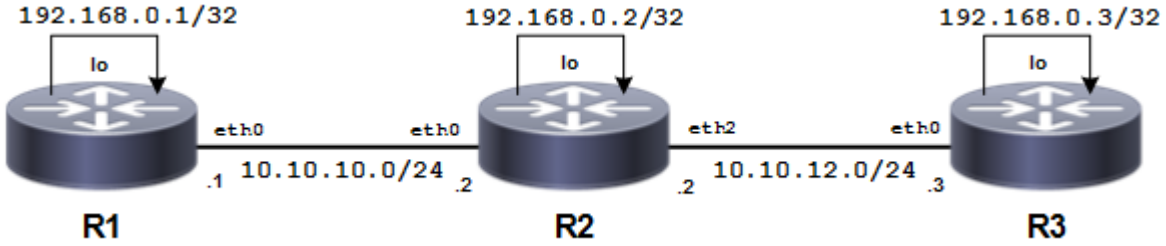


Figure 1-49: Basic Static Route

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
```

CHAPTER 2 RIP

This chapter contains basic Router Information Protocol (RIP) configuration examples.

Enable RIP

This example shows the minimum configuration required to enable RIP on an interface. R1 and R2 are two routers connecting to network 10.10.11.0/24. R1 and R2 are also connected to networks 10.10.10.0/24 and 10.10.12.0/24, respectively. To enable RIP, first define the RIP routing process, then associate a network with the routing process.

Topology

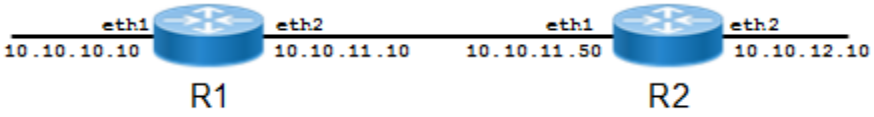


Figure 2-50: Enable RIP Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24` `(config-router)#network 10.10.11.0/24`	Associate networks with the RIP process.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.11.0/24` `(config-router)#network 10.10.12.0/24`	Associate networks with the RIP process.

Validation

show ip rip, show running-config, show ip protocols rip, show ip rip interface, show ip route

R1

```
#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
Rc 10.10.11.0/24                           1                  eth2
```

```
#show running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.10.10/24
!
interface eth2
 ip address 10.10.11.10/24
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 14 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:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
    eth2             2     2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#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"
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       10.10.11.0/24 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       192.168.0.2/32 is directly connected, lo
```

R2

```
#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.11.0/24                           1                  eth1
Rc 10.10.12.0/24                           1                  eth2

2#show running-config
!
no service password-encryption
!
hostname rtr2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.3/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.183/24
!
interface eth1
 ip address 10.10.11.50/24
!
interface eth2
 ip address 10.10.12.10/24
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
!
line con 0
 login
line vty 0 39
```

```
 login
!
end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 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:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
    eth2             2     2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#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"
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       10.10.11.0/24 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
C       192.168.0.3/32 is directly connected, lo
```

Specify RIP Version

Configure a router to receive and send specific versions of packets on an interface. In this example, router R2 is configured to receive and send RIP version 1 and version 2 information on both eth1 and eth2 interfaces.

Topology

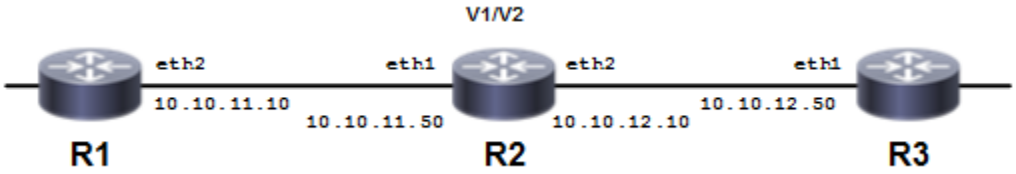


Figure 2-51: RIP Version Topology

R2

`#configure terminal`	Enter configure mode
`(config)#router rip`	Enable the RIP routing process
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip rip send version 1 2`	Send RIP version 1 and version 2 packets out this interface
`(config-if)#ip rip receive version 1 2`	Receive RIP version 1 and version 2 packets from this interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip rip send version 1 2`	Send RIP version 1 and version 2 packets out this interface
`(config-if)#ip rip receive version 1 2`	Receive RIP version 1 and version 2 packets from this interface

Validation

R2

```
#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default
```

```
   Network            Next Hop         Metric From            If     Time
Rc 10.10.11.0/24                           1                  eth1
Rc 10.10.12.0/24                           1                  eth2

#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.11.50/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth2
 ip address 10.10.12.10/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip protocols rip
```

```
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 29 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:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             1 2   1 2
    eth2             1 2   1 2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.10           120  00:00:31               0           0
    10.10.12.50           120  00:00:08               0           0
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#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"
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       10.10.11.0/24 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
C       192.168.0.2/32 is directly connected, lo
```

Authentication with a Single Key

OcNOS RIP provides a choice of configuring authentication with a single key or with multiple keys. This example shows authenticating routing information exchange using a single key.

Topology

Routers R1 and R2 are running RIP and exchanging routing updates. To configure single-key authentication on R1, specify an interface, then define a key or password for that interface. Next, specify an authentication mode. Any receiving RIP packet on this specified interface should have the same string as the password. For an exchange of updates between R1 and R2, define the same password and authentication mode on R2.

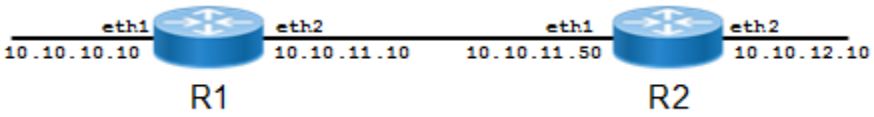


Figure 2-52: Single-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (`eth1`) for authentication.
`(config-if)#ip rip authentication string ABC`	Specify the authentication string (`ABC`) for this interface.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to be MD5.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.

(config)#interface eth2	Specify the interface (eth2) for authentication.
(config-if)#ip rip authentication string ABC	Specify the authentication string (ABC) on this interface.
(config-if)#ip rip authentication mode md5	Specify the authentication mode to be MD5.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
#show running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode md5
 ip rip authentication string 0x5c5b790e25d29287
!
interface eth2
 ip address 10.10.11.10/24
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
```

```
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.10.11.0/24                           1                  eth2
R  10.10.12.0/24      10.10.10.50          2 10.10.10.50      eth1   02:33
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo
R  192.168.0.2/32     10.10.10.50          2 10.10.10.50      eth1   02:33

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 26 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.10.50           120  00:00:31               0           0
  Number of routes (including connected): 6
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
```

```
  RIP is not enabled on this interface

#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"
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       10.10.11.0/24 is directly connected, eth2
R       10.10.12.0/24 [120/2] via 10.10.10.50, eth1, 00:04:05
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
R       192.168.0.2/32 [120/2] via 10.10.10.50, eth1, 00:04:05
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.12.50/24
!
```



```
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode md5
 ip rip authentication string 0x5c5b790e25d29287
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
R  10.10.11.0/24      10.10.10.10          2 10.10.10.10      eth2   02:58
C  10.10.12.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
R  192.168.0.1/32     10.10.10.10          2 10.10.10.10      eth2   02:58
C  192.168.0.2/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.10.10           120  00:00:01               0           0
  Number of routes (including connected): 6
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
```

```
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is up, line protocol is up
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#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"
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, eth2
R       10.10.11.0/24 [120/2] via 10.10.10.10, eth2, 00:07:36
C       10.10.12.0/24 is directly connected, eth1
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
R       192.168.0.1/32 [120/2] via 10.10.10.10, eth2, 00:07:36
C       192.168.0.2/32 is directly connected, lo
```

Text Authentication with Multiple Keys

This example illustrates text authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or set of keys) that will be used for authentication on each interface, and the authentication mode to use.

R1 receives all packets that contain any key string that matches one of the key strings included in the specified key chain (within the accept lifetime) on that interface. The key ID is not considered for matching. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap. This will accommodate different time setup on machines. However, the send lifetime is not required to overlap, and IP Infusion Inc. recommends configuring no overlapping for the send lifetime.

Topology

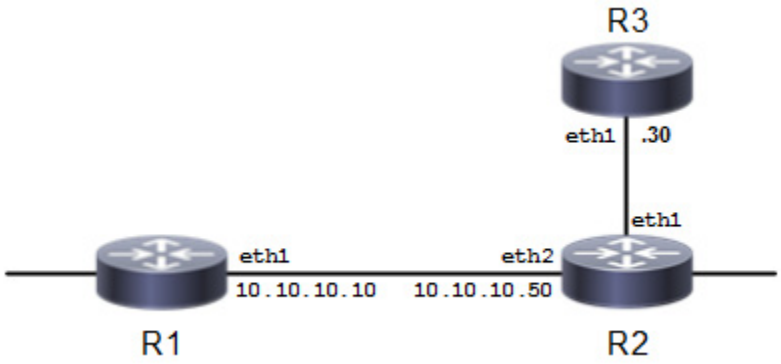


Figure 2-53: Multiple-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain SUN`	Enter Keychain management mode to add keys to the key chain `SUN`.
`(config-keychain)#key 10`	Add authentication key ID (`10`) to the key chain `SUN`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain-key)#exit`	Exit Keychain-Key mode, and return to Keychain mode.
`(config-keychain)#key 20`	Add another authentication key (`20`) to the key chain `SUN`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify interface `eth1` as the interface you want to configure.
`(config-if)#ip rip authentication key chain SUN`	Enable RIPv2 authentication on `eth1` interface and specify the key chain `SUN` to use for authentication.
`(config-if)#ip rip authentication mode text`	Specify text authentication mode to use for RIP packets. This step is optional, because text is the default mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain MOON`	Enter Keychain management mode to add keys to the key chain `MOON`.
`(config-keychain)#key 30`	Add authentication key ID (`30`) to the key chain `MOON`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain)#key 40`	Add another authentication key (`40`) to the key chain `MOON`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.
`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify interface `eth2` as the interface you want to configure.
`(config-if)#ip rip authentication key chain MOON`	Enable RIPv2 authentication on the `eth1` interface, and specify the key chain `MOON` to use for authentication.
`(config-if)#ip rip authentication mode text`	Specify the authentication mode to use for RIP packets. This step is optional, because text is the default mode.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
key chain SUN
 key 10
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 20
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode text
 ip rip authentication key-chain chain SUN
!
interface eth2
!
router rip
 network 10.10.10.0/24
```

```
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 16 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2      chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is down, line protocol is down
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```



```
#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"
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       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.1/32 is directly connected, lo
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
key chain MOON
 key 30
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 40
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
```

```
 ip address 10.12.4.108/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode text
 ip rip authentication key-chain chain MOON
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
C  10.12.4.0/24                            1                  eth0
C  192.168.0.2/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2      chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
```

```
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is down, line protocol is down
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#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"
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, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.2/32 is directly connected, lo
```

MD5 Authentication with Multiple Keys

This example illustrates the MD5 authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Then, set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or the set of keys) that will be used for authentication on the interface, and the authentication mode to use. Configure R2 and R3 to have the same key ID and key string as R1 for the time that updates are to be exchanged.

In MD5 authentication, both the key ID and key string are matched for authentication. R1 will receive only packets that match both the key ID and the key string in the specified key chain (within the accept lifetime) on that interface. In the following example, R2 has the same key ID and key string as R1. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap; however, the send lifetime should not overlap.

Topology

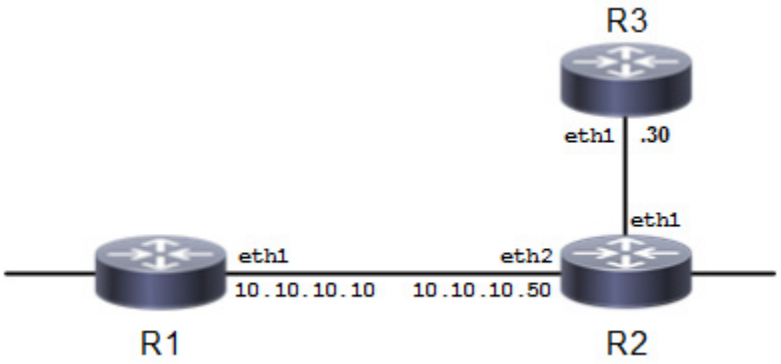


Figure 2-54: MD5 Multiple-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain SUN`	Enter Keychain management mode to add keys to the key chain `SUN`.
`(config-keychain)#key 1`	Add authentication key ID (`1`) to the key chain `SUN`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain-key)#exit`	Exit Keychain-Key mode, and return to Keychain mode.
`(config-keychain)#key 2`	Add another authentication key (`2`) to the key chain `SUN`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.
`#configure terminal`	Enter configure mode.

(config)#interface eth1	Specify interface eth1 as the interface you want to configure.
(config-if)#ip rip authentication key chain SUN	Enable RIPv2 authentication on the eth1 interface, and specify the key chain SUN to use for authentication.
(config-if)#ip rip authentication mode md5	Specify MD5 authentication mode to use for RIP packets.

R2

#configure terminal	Enter configure mode.
(config)#router rip	Define a RIP routing process, and enter Router mode.
(config-router)#network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
(config-router)#redistribute connected	Enable redistributing from connected routes.
(config-router)#exit	Exit router mode.
(config)#key chain MOON	Enter Keychain management mode to add keys to the key chain MOON.
(config-keychain)#key 1	Add authentication key ID (1) to the key chain MOON.
(config-keychain-key)#key-string ABC	Specify a password (ABC) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003	Specify the time period during which the authentication key can be received. In this case, key string ABC can be received from noon of March 2 to 2 pm March 7, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003	Specify the time period during which the authentication key can be sent. In this case, key string ABC can be sent from noon of March 2 to noon of March 7, 2003.
(config-keychain)#key 2	Add another authentication key (2) to the key chain MOON.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003	Specify the time period during which the authentication key can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003	Specify the time period during which the authentication key can be sent. In this case, key string Earth can be sent from noon of March 7 to noon of March 12, 2003.
(config-keychain-key)#end	Enter Privileged Exec mode.
#configure terminal	Enter configure mode.
(config)#interface eth2	Specify interface eth2 as the interface you want to configure.
(config-if)#ip rip authentication key chain MOON	Enable RIPv2 authentication on the eth1 interface, and specify the key chain MOON to use for authentication.
(config-if)#ip rip authentication mode md5	Specify the authentication mode to use for RIP packets.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
key chain SUN
 key 1
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 2
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode md5
 ip rip authentication key-chain chain SUN
!
interface eth2
!
router rip
 network 10.10.10.0/24
```

```
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 19 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2      chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is down, line protocol is down
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
key chain MOON
 key 1
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 2
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
ip address 10.12.4.108/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode md5
 ip rip authentication key-chain chain MOON
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
```

```
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
C  10.12.4.0/24                            1                  eth0
R  192.168.0.1/32     10.10.10.10         16 10.10.10.10     eth2   01:29
C  192.168.0.2/32                          1                  lo


#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 9 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
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2      chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 4
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is down, line protocol is down
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```

CHAPTER 3 RIPng

This chapter contains a basic RIPng configuration example.

Topology

The diagram shows the minimum configuration required to enable RIPng on an interface. R1 and R2 are two routers connected to network 3ffe:11::/64. To enable RIPng, first define the RIPng routing process, then enable RIPng on each interface.

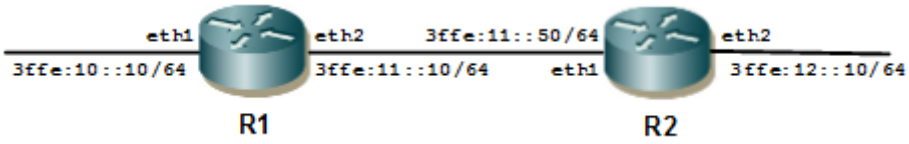


Figure 3-55: RIPng Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth2`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#router ipv6 rip`	Define a RIPng routing process, and enter Router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth2`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#router ipv6 rip`	Define a RIPng routing process, and enter Router mode.

Validation

show ipv6 rip

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

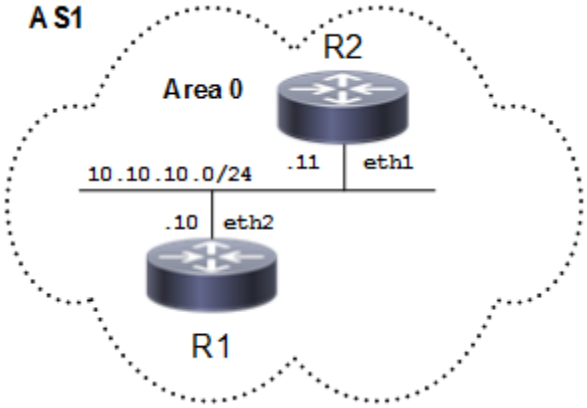


Figure 4-56: Basic OSPF Topology

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

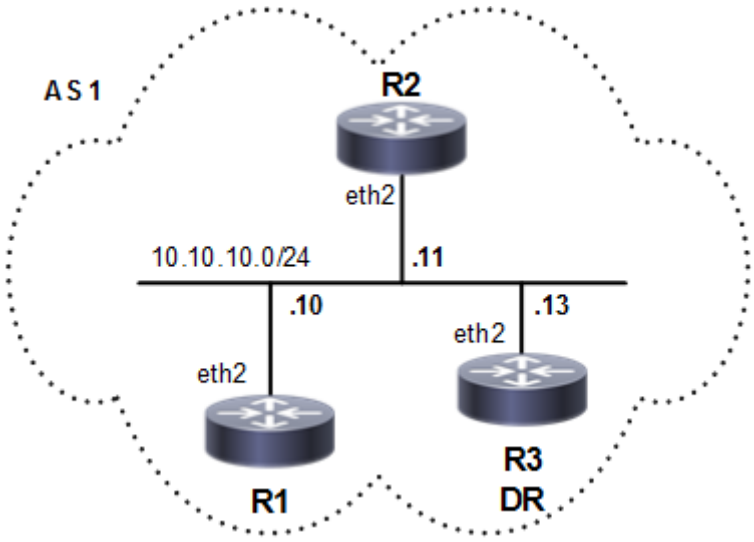


Figure 4-57: Set OSPF Priority

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
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end
```

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
!
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
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

#sh 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#sh 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

```
#sh running-config
!
```

```
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

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
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

#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
10.12.26.88       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
```

```
#sh 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

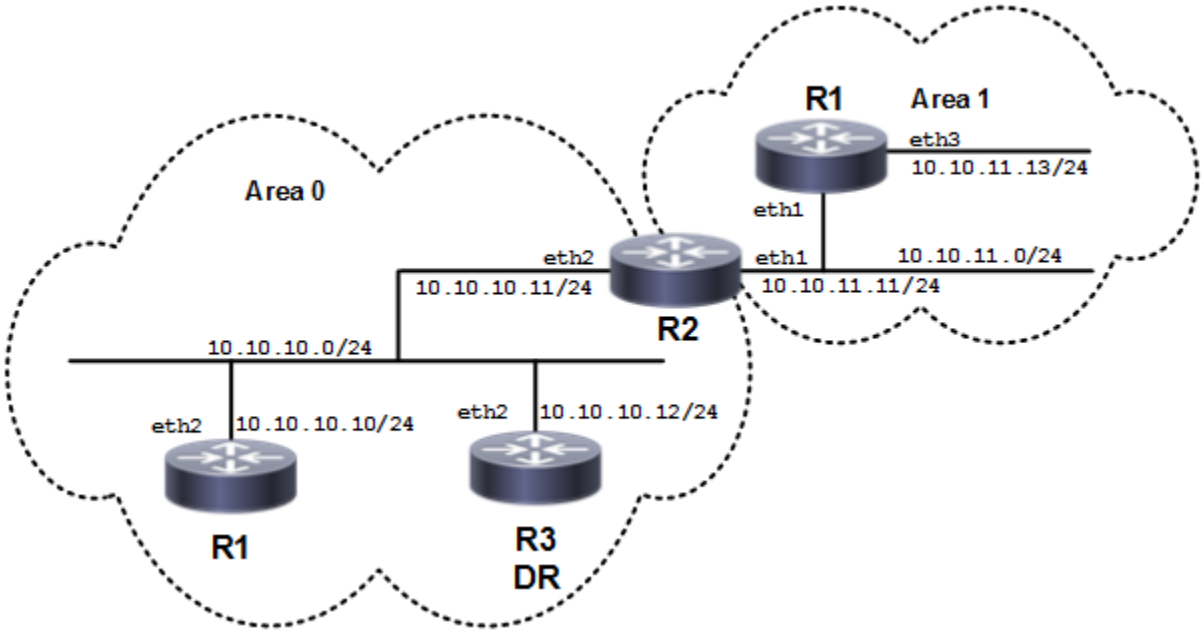


Figure 4-58: OSPF ABR Topology

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
 cspf disable-better-protection
!
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

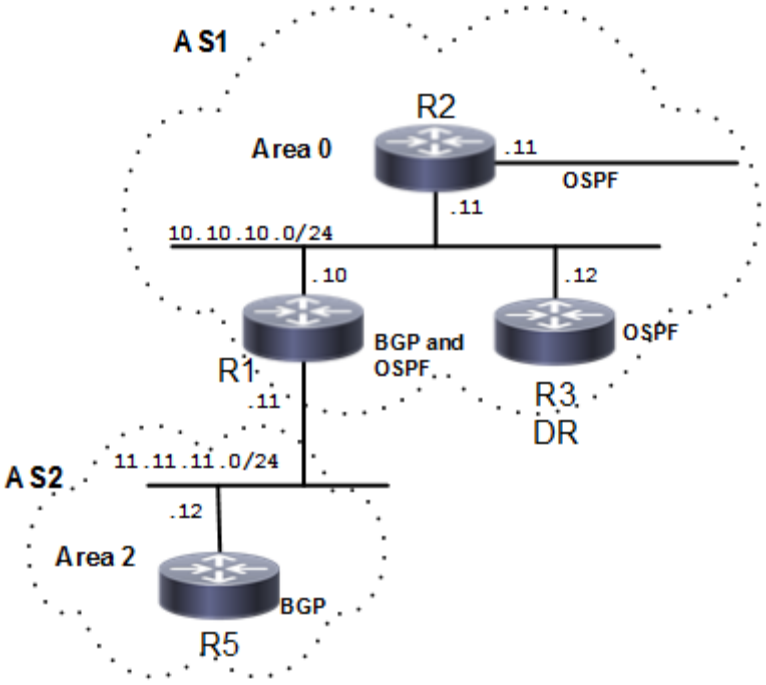


Figure 4-59: Redistribute Routes

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

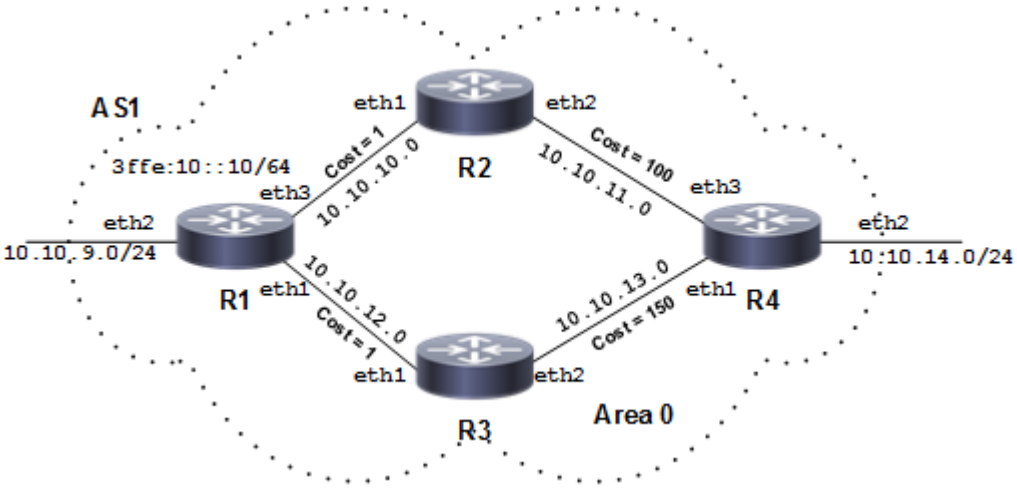


Figure 4-60: Configure Cost Topology

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

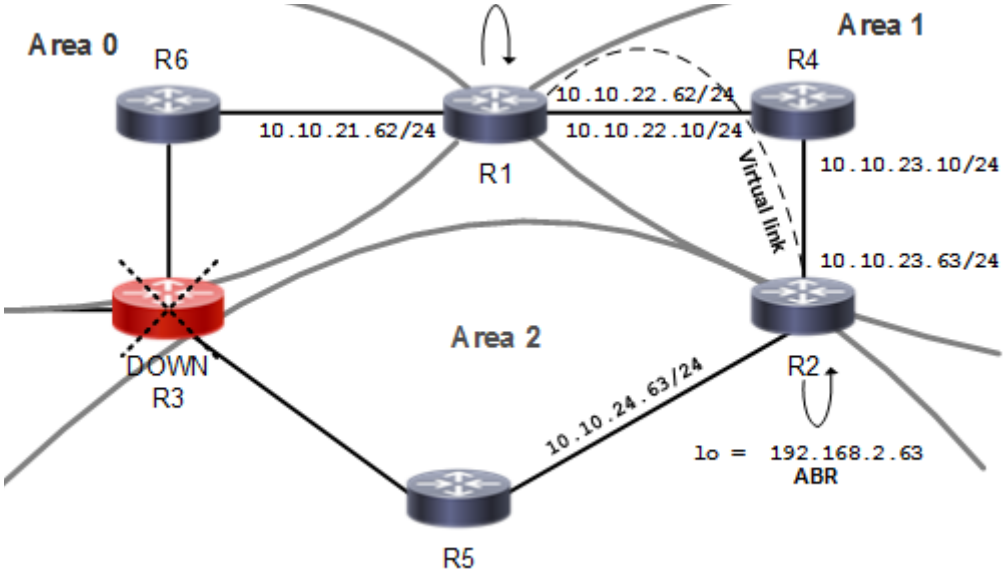


Figure 4-61: Virtual Links Topology

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

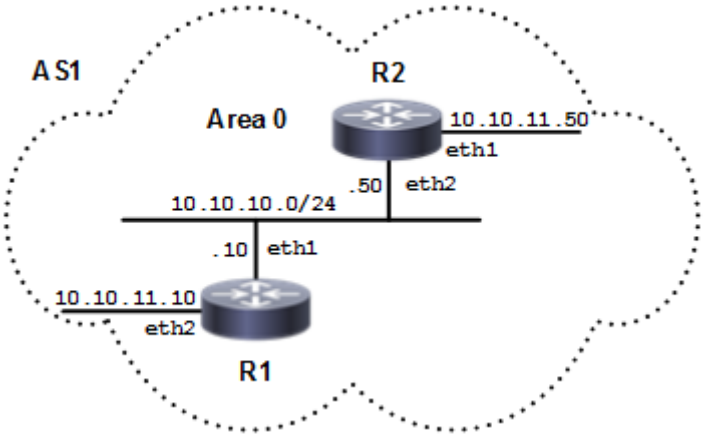


Figure 4-62: OSPF Authentication Topology

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 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 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 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 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
 cspf disable-better-protection
!
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
 cspf disable-better-protection
!
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

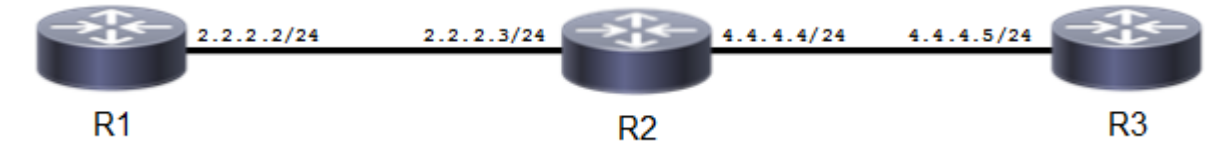


Figure 4-63: Multiple OSPF Instances

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
 cspf disable-better-protection
!
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
cspf disable-better-protection
```

```
!
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
 cspf disable-better-protection
!
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

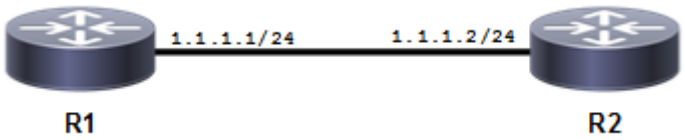


Figure 4-64: Multiple Instances on the Same Subnet

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

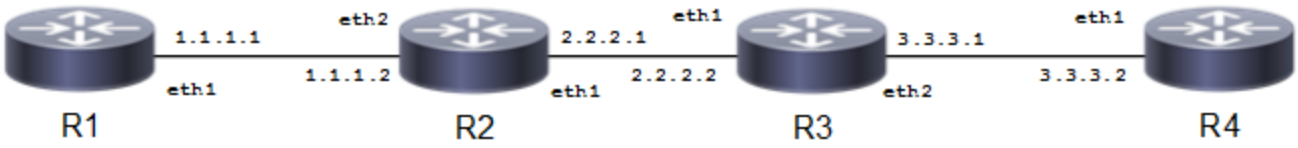


Figure 4-65: One Subnet with Multiple OSPF Areas

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

show ip ospf multi-area-adjacencies, show ip ospf neighbor, show ip ospf route, show ip route

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.

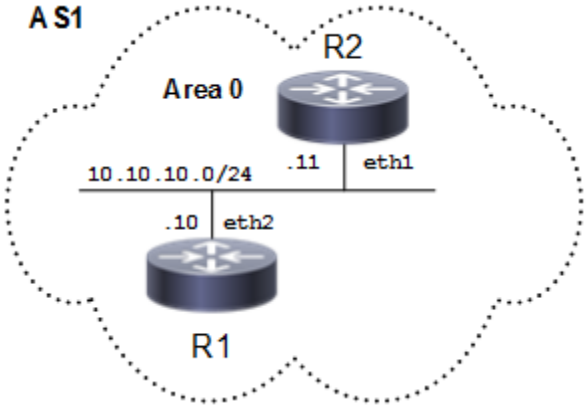


Figure 4-66: Basic OSPF Topology

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

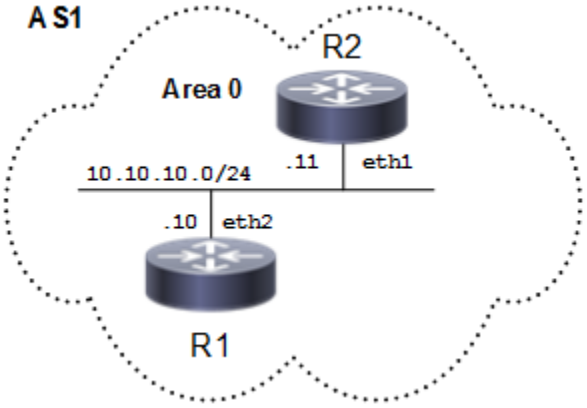


Figure 4-67: Basic OSPF Topology

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
```

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

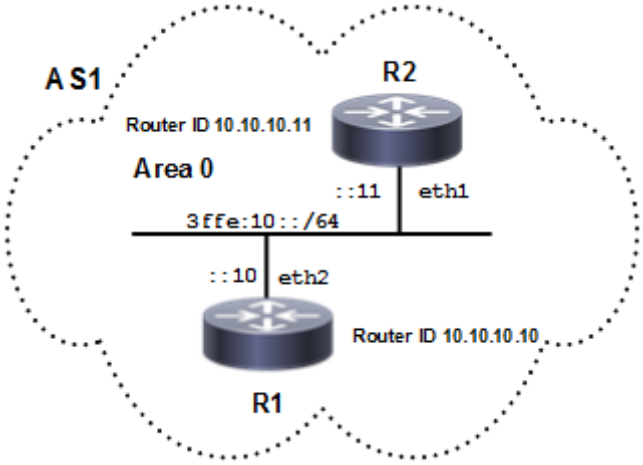


Figure 5-68: Basic OSPFv3 Topology

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

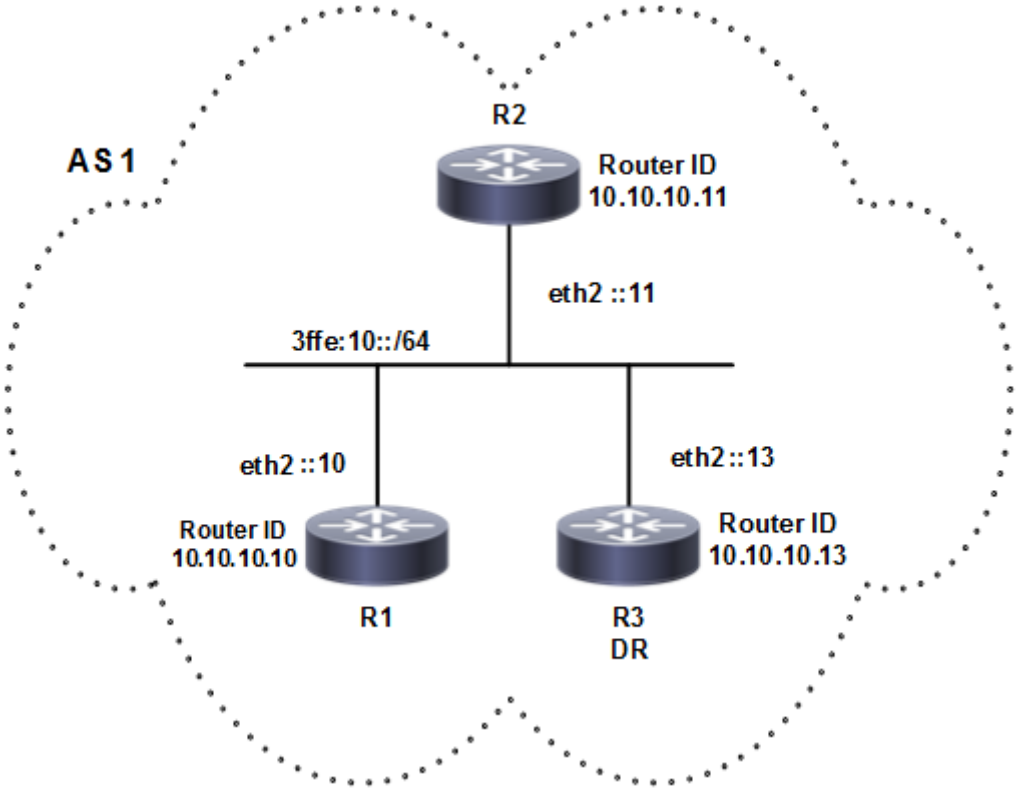


Figure 5-69: OSPFv3 Set Priority

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

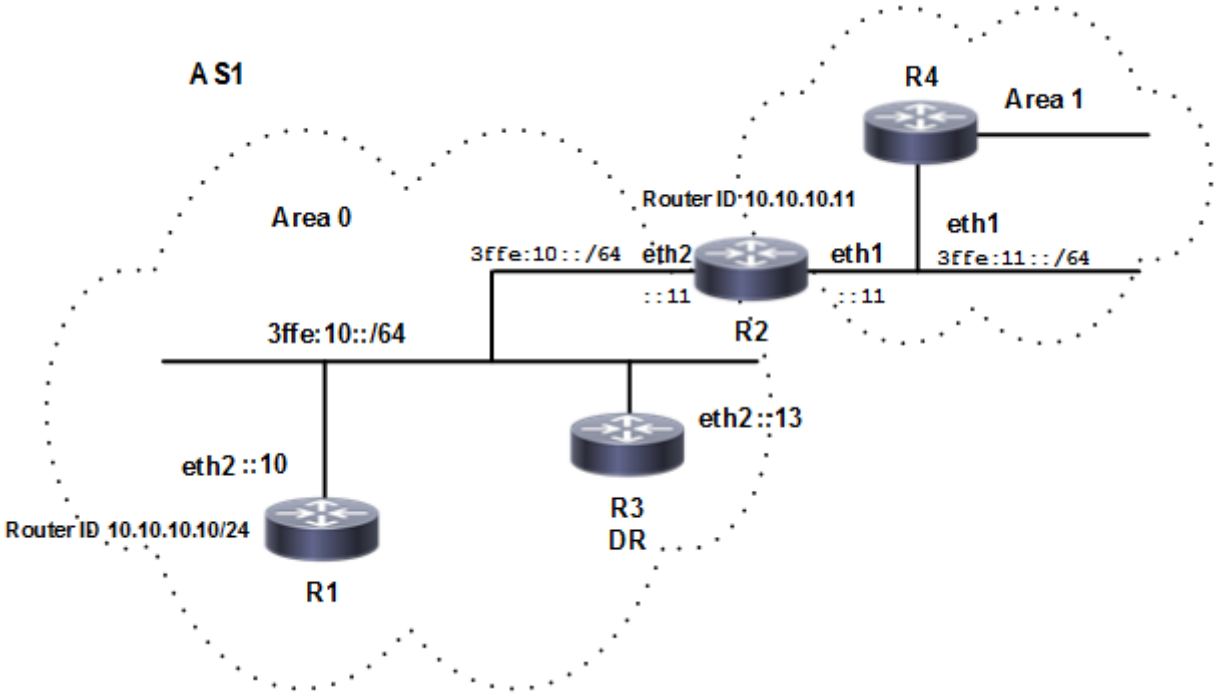


Figure 5-70: OSPFv3 Area Border Router

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)`.

Validation

R2

```
R2S#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DROther    00:00:33    eth1       0
10.10.10.12       1   Full/DR         00:00:31    eth1       0
10.10.10.13       1   Full/DR         00:00:36    eth2       0


R2S#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         10.10.10.10      171       0x80000001 0xaa25      1
0.0.0.3         10.10.10.11      139       0x80000001 0x87eb      1
0.0.0.3         10.10.10.12      132       0x80000001 0x2032      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.11      139       0x80000001 0xb466      1
0.0.0.4         10.10.10.13      130       0x80000001 0x8c5b      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       83       0x80000005 0xbae6      1
0.0.0.0         10.10.10.11       82       0x80000005 0xb7e7      1
0.0.0.0         10.10.10.12       87       0x80000003 0xb2ee      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.12       87       0x80000002 0xacad

                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      134       0x80000002 0xfd5e

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.12       86       0x80000001 0xc954      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       83       0x80000003 0x57e0
0.0.0.3         10.10.10.11       77       0x80000004 0x81b3
0.0.0.3         10.10.10.12       87       0x80000003 0xaf84

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.11       89       0x80000003 0xf1ac      1
0.0.0.0         10.10.10.13       85       0x80000003 0xe2ba      1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13       90       0x80000001 0x067e

                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      134       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         10.10.10.13       84       0x80000001 0x0eec      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.11       89       0x80000002 0xb75c
0.0.0.4         10.10.10.13       89       0x80000002 0xdd33


R2S#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          B  --
10.10.10.12             1          10.10.10.12          eth1

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.11          B  --
10.10.10.13             1          10.10.10.13          eth2


R2S#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, 00:02:52
C      3ffe:10::/64 via ::, eth1, 00:02:51
C      6ffe::/64 via ::, eth2, 00:02:51
C      fe80::/64 via ::, eth2, 00:02:52


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
C  6ffe::/64                                        1
     directly connected, eth2, Area 0.0.0.1
```

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

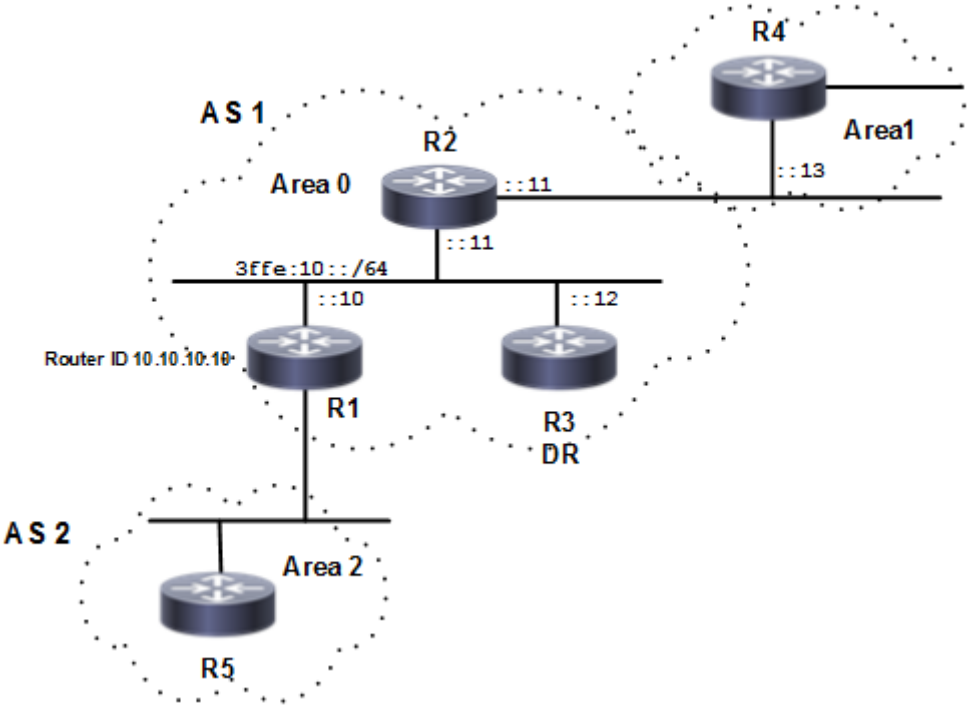


Figure 5-71: OSPFv3 Redistribute Routes

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)#redistribute bgp`	Specify redistributing routes from the other routing protocol (BGP) into OSPFv3.
`(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

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              00:00:40         eth1       0
10.10.10.12       1   Full/DROther    00:00:40          eth1       0
10.10.10.13       1   Full/Backup      00:00:33          eth2       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
0.0.0.3           10.10.10.10      364       0x80000002    0x21a3      1
0.0.0.3           10.10.10.11     1046       0x80000001   0xa3f6       1
0.0.0.3           10.10.10.12     1018       0x80000001   0xd00e      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#               CkSum     Prefix
0.0.0.4           10.10.10.11     1046      0x80000001   0xc0b0      1
0.0.0.3           10.10.10.13      985       0x80000001   0x61e4      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     1007       0x80000005   0x9709      1
0.0.0.0           10.10.10.11     1003       0x80000004   0x8d15      1
0.0.0.0           10.10.10.12     1002       0x80000004   0x841e      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.3           10.10.10.10     1007       0x80000002   0xc497

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.1           10.10.10.10      355       0x80000003   0x511b
0.0.0.1           10.10.10.11      1041     0x80000002   0x9cdf

                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     1006       0x80000002 0x56da      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      1007      0x80000003      0xc881
```

```
0.0.0.3           10.10.10.11      1003      0x80000003      0xf453
0.0.0.3           10.10.10.12      1002      0x80000003      0x2125

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#              CkSum     Link
0.0.0.0           10.10.10.11      973       0x80000004   0xc3db      1
0.0.0.0           10.10.10.13      973       0x80000003   0xa8f7       1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.4           10.10.10.11      973       0x80000001     0x1a6c

                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     1041      0x80000002     0xeba0
0.0.0.2           10.10.10.11      969       0x80000002     0x4921

                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     1019      0x80000001    0x9c16

                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      972       0x80000001  0x9b83      1
Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.4           10.10.10.11      973       0x80000002    0x47ee
0.0.0.3           10.10.10.13      973       0x80000002    0xa989


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        EB  1          10.10.10.10         eth1
10.10.10.11         B  --
10.10.10.12         1               10.10.10.12          eth1

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop            Interface
10.10.10.11         B  --
10.10.10.13         1                 10.10.10.13          eth2


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::/64                                         1
     directly connected, eth1, Area 0.0.0.0
C  4ffe::/64                                         1
     directly connected, eth2, Area 0.0.0.1
IA 5ffe::/64                                         2
     via fe80::5054:ff:fe58:fc20, eth1, 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, 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, 00:44:22
C      3ffe::/64 via ::, eth1, 00:18:00
C      4ffe::/64 via ::, eth2, 00:18:00
O IA   5ffe::/64 [110/2] via fe80::5054:ff:fe58:fc20, eth1, 00:17:32
C      fe80::/64 via ::, eth2, 00:44:22
```

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           00:00:37         eth1       0
10.10.10.11       1   Full/Backup     00:00:34          eth1       0


R3#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.12) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age        Seq#               CkSum    Prefix
0.0.0.3           10.10.10.10     459        0x80000002     0x21a3      1
0.0.0.3           10.10.10.11    1142       0x80000001     0xa3f6      1
0.0.0.3           10.10.10.12    1111       0x80000001     0xd00e      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    1103       0x80000005     0x9709      1
0.0.0.0           10.10.10.11    1099       0x80000004     0x8d15      1
0.0.0.0           10.10.10.12    1096       0x80000004     0x841e      1

                Network-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.3           10.10.10.10     1103       0x80000002    0xc497

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#                CkSum
0.0.0.1           10.10.10.10      450        0x80000003     0x511b
0.0.0.1           10.10.10.11     1137       0x80000002     0x9cdf

                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     1101       0x80000002   0x56da      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     1103       0x80000003    0xc881
0.0.0.3           10.10.10.11     1099       0x80000003    0xf453
0.0.0.3           10.10.10.12     1096       0x80000003    0x2125

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        EB  1          10.10.10.10            eth1
10.10.10.11         B  1          10.10.10.11             eth1
10.10.10.12            --

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
C  3ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0
IA 4ffe::/64                                         2
     via fe80::5054:ff:fe5b:1034, eth1, Area 0.0.0.0
IA 5ffe::/64                                         2
     via fe80::5054:ff:fe58:fc20, 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, 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, 00:45:05
```

```
C       3ffe::/64 via ::, eth1, 00:18:53
O IA    4ffe::/64 [110/2] via fe80::5054:ff:fe5b:1034, eth1, 00:18:39
O IA    5ffe::/64 [110/2] via fe80::5054:ff:fe58:fc20, eth1, 00:18:39
C       fe80::/64 via ::, eth2, 00:45:05
```

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

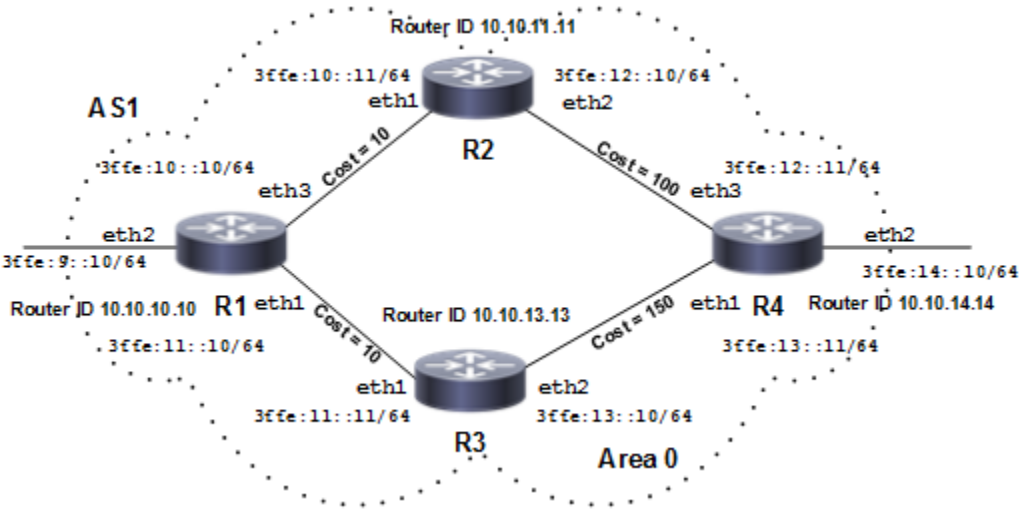


Figure 5-72: Configure Cost OSPFv3

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.
`(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)`.

`#configure terminal`	Enter configure mode.
`(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

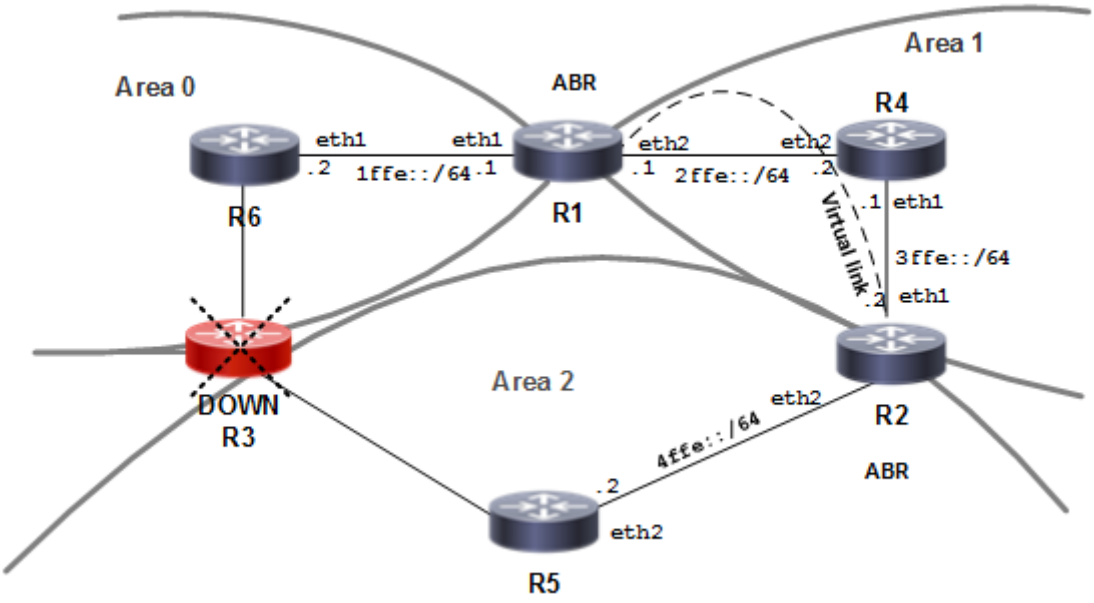


Figure 5-73: OSPFv3 Virtual Links

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

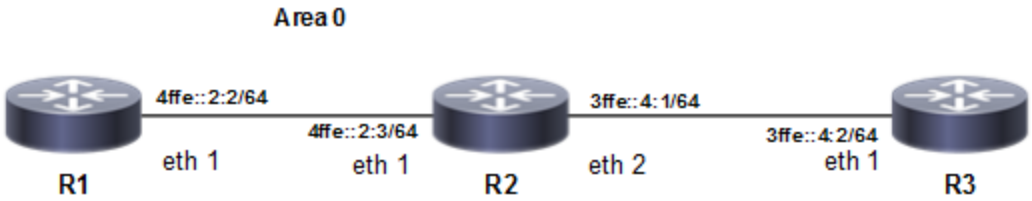


Figure 5-74: Multiple OSPFv3 Instances

Enable OSPFv3 on an Interface

This example shows how to enable OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to network 4ffe::2:/64.

R1

`(config)#router ipv6 ospf 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(config-router)#router-id 151.151.151.151`	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 10`	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 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(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 4ffe::2:3/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 10`	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

```
#show running-config
!
```

```
!Last configuration change at 11:33:37 EDT Tue Mar 12 2019 by ocnos
!
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
$1$qLd1Mdn0$rrz9r.00v.xla6xd2KDw91
feature rsyslog
!
interface lo
 ip address 127.0.0.1/8
 ip address 151.151.151.151/32 secondary
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.20.2/24
!
interface eth1
 ipv6 address 4ffe::2:2/64
 ipv6 router ospf area 0.0.0.0 tag 10
!
interface eth2
!
interface eth3
!
router ipv6 ospf 10
 router-id 151.151.151.151
 capability te
 capability cspf
!
line con 0
 login
line vty 0 39
 login
!
end

#show ipv6 interface brief
Interface            IPv6-Address                                    Admin-
Status
eth3                 fe80::5054:ff:fe44:c9f9                         [up/up]
eth2                 fe80::5054:ff:fe49:d3ec                         [up/up]
eth1                 4ffe::2:2
                     fe80::5054:ff:fef3:2245                         [up/up]
eth0                 fe80::5054:ff:fec8:55b1                         [up/up]
lo                   ::1                                             [up/up]
```

```
#show ipv6 ospf route
OSPFv3 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

   Destination                                      Metric
     Next-hop
IA 3ffe::/64                                           2
     via fe80::5054:ff:fe22:ed80, eth1, Area 0.0.0.0
C  4ffe::/64                                           1
     directly connected, eth1, Area 0.0.0.0

# show ipv6 ospf neighbor
OSPFv3 Process (10)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.14.14       1   Full/DROther    00:00:34    eth1       0
152.152.152.152   1   Full/DR         00:00:34    eth1       0
```

R2

```
#show running-config
!
!Last configuration change at 12:34:42 EDT Tue Mar 12 2019 by ocnos
!
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 $1$YLcV3GI1$TV02h9a0/
z2oPtHU95f02/
feature rsyslog
!
interface lo
 ip address 127.0.0.1/8
 ip address 152.152.152.152/32 secondary
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.20.3/24
!
interface eth1
 ipv6 address 4ffe::2:3/64
 ipv6 router ospf area 0.0.0.0 tag 10
!
```

```
interface eth2
!
router ipv6 ospf 10
 router-id 152.152.152.152
 capability te
 capability cspf
!
line con 0
 login
line vty 0 39
 login
!
end

#show ipv6 interface brief
Interface            IPv6-Address                                    Admin-
Status
eth2                 fe80::5054:ff:fe39:f13f                         [up/up]
eth1                 4ffe::2:3
                     fe80::5054:ff:febc:57d                          [up/up]
eth0                 fe80::5054:ff:fea2:3f3                          [up/up]
lo                   ::1                                             [up/up]

# show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
IA 3ffe::/64                                        2
     via fe80::5054:ff:fe22:ed80, eth1, Area 0.0.0.0
C  4ffe::/64                                        1
     directly connected, eth1, Area 0.0.0.0

# show ipv6 ospf neighbor
OSPFv3 Process (10)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.14.14       1   Full/DROther    00:00:39    eth1       0
151.151.151.151   1   Full/Backup     00:00:40    eth1       0
```

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)#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
O  3ffe:12::/64                                       1
     directly connected, eth2, Area 0.0.0.0
O  3ffe:13::/64                                       2
     via fe80::a00:27ff:fe01:c94d, 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
O  3ffe:12::/64                                       1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:13::/64                                       2
     via fe80::a00:27ff:fe01:c94d, 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 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 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)#redistribute connected	Redistribute co routes to instance 15.
(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.
(config-router)#redistribute connected	Redistribute connected routes to instance 5.

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, 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 `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(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 5 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `5`.

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

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                                        1/20
     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     00:00:37    eth1       0
```

Redistribute with 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 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 `15` routes as type `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(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 with type 2.
(config-router)#redistribute connected	Redistribute instance 15 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 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
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 I
D
159.159.159.159   1   Full/Backup     00:00:36    eth1       0
```

Redistribute with Route-Map Option

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 route-map 1`	Redistribute instance `5` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(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::a00:27ff:fef9:2432, eth1
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 I
D
149.149.149.149   1   Full/DR         00:00:34    eth1       0
```

R2

```
R2#sh 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/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::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/DR         00:00:34    eth1       0
R3#
```

Graceful Restart

The possibility of maintaining a router's data forwarding capability while the router's control software restarts is called graceful restart or non-stop forwarding. After the router restarts and reloads, it must change its OSPF processing until it re-establishes full adjacencies with all its former fully adjacent neighbors. The time period between the restart/reload and re-establishment of adjacencies is called the grace period.

Essentially, the OSPF procedure for graceful restart is as follows:

- The router attempting a graceful restart originates link-local Opaque-LSAs, called Grace-LSAs, announcing its intention to perform a graceful restart within a specified amount of time (grace period).
- During the grace period, neighbors continue to announce the restarting router in their LSAs as if it were fully adjacent (OSPF neighbor state Full), but only if the network topology remains static (the contents of the LSAs in the link-state database that have LS types 1-5 and 7 remain unchanged, and periodic refreshes are allowed).

Topology

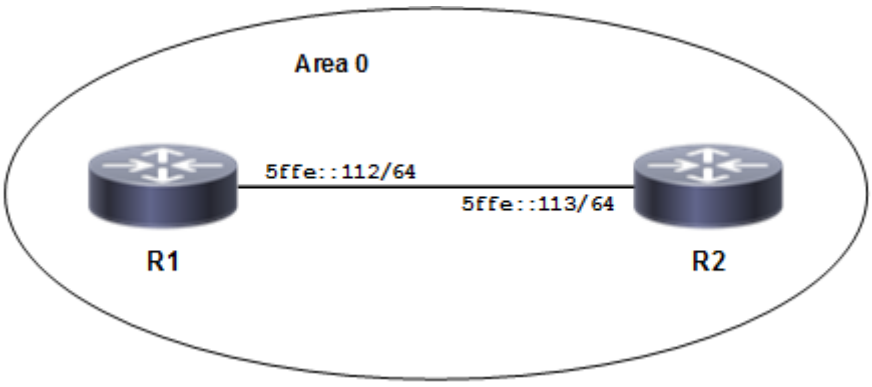


Figure 5-75: OSPFv3 Graceful Restart

Configure R1 for Graceful Restart

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 5ffe::112/64`	Assign the IPv6 address to the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Configure the interface for OSPFv3 on area 0.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	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)#capability restart graceful`	Enable graceful restart capability.
`(config-router)#end`	Exit Configure mode and enter Privileged Exec mode.
`#write`	Save the configuration.
`#restart ipv6 ospf graceful grace-period 200`	Restart OSPFv3 with a 200-second grace period, so that the neighbor maintains adjacency and preserves the routes for 200 seconds.

Configure R2 as Restart Helper

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 5ffe::113/64`	Assign the IPv6 address to the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Configure the interface for OSPFv3 on area 0.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	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)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper max-grace-period 300`	Configure R2 to act as the helper when the grace period is less than 300.

Remove Helper Configuration from R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	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)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper never`	Configure R2 to not work as the helper.

Make R2 Helper when Restart Reason is Reload

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	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)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper only-reload`	Configure R2 to work as the helper only when the restart reason is reload.

Make R2 Helper when Restart Reason is Upgrade

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	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)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper only-upgrade`	Configure R2 to work as the helper only when the restart reason is upgrade.

Validation

R1 After Configuring Graceful Restart

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:39    eth1       0


R1#show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, 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, 02:02:28
C       5ffe::/64 via ::, eth1, 00:23:16
C       fe80::/64 via ::, eth1, 01:25:04
K       ff00::/8 [0/256] via ::, eth0, 01:25:05


rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R1 After Graceful Restart (after starting ospf6d daemon manually)

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:37    eth1       0


rtr1#show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, 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, 02:02:28
C       5ffe::/64 via ::, eth1, 00:23:16
C       fe80::/64 via ::, eth1, 01:25:04
K       ff00::/8 [0/256] via ::, eth1, 01:25:05


rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R2 Before Graceful Restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:40    eth1       0
```

```
R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:40    eth1       0
R2#
R2#show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, 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, 01:54:20
C      5ffe::/64 via ::, eth1, 00:12:16
C      fe80::/64 via ::, eth2, 01:17:21
K      ff00::/8 [0/256] via ::, eth1, 01:19:12


R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

R2 During graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:02:25*    eth1       0


R2#show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, 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, 01:57:26
C      5ffe::/64 via ::, eth1, 00:15:22
C      fe80::/64 via ::, eth2, 01:20:27
K      ff00::/8 [0/256] via ::, eth1, 01:22:18


R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)

                Grace-LSA (Interface eth1)

  LS age: 65
  LS Type: Grace LSA
  Link State ID: 0.0.0.3
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0x1660
  Length: 36

      Grace Period: 200
      Restart Reason:
           Software Restart
```

R2 After graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:34    eth1       0



R2#show ipv6 ospf route
OSPFv3 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

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, 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, 02:07:14
C       5ffe::/64 via ::, eth1, 00:25:10
C       fe80::/64 via ::, eth2, 01:30:15
K       ff00::/8 [0/256] via ::, eth2, 01:30:17

R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

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

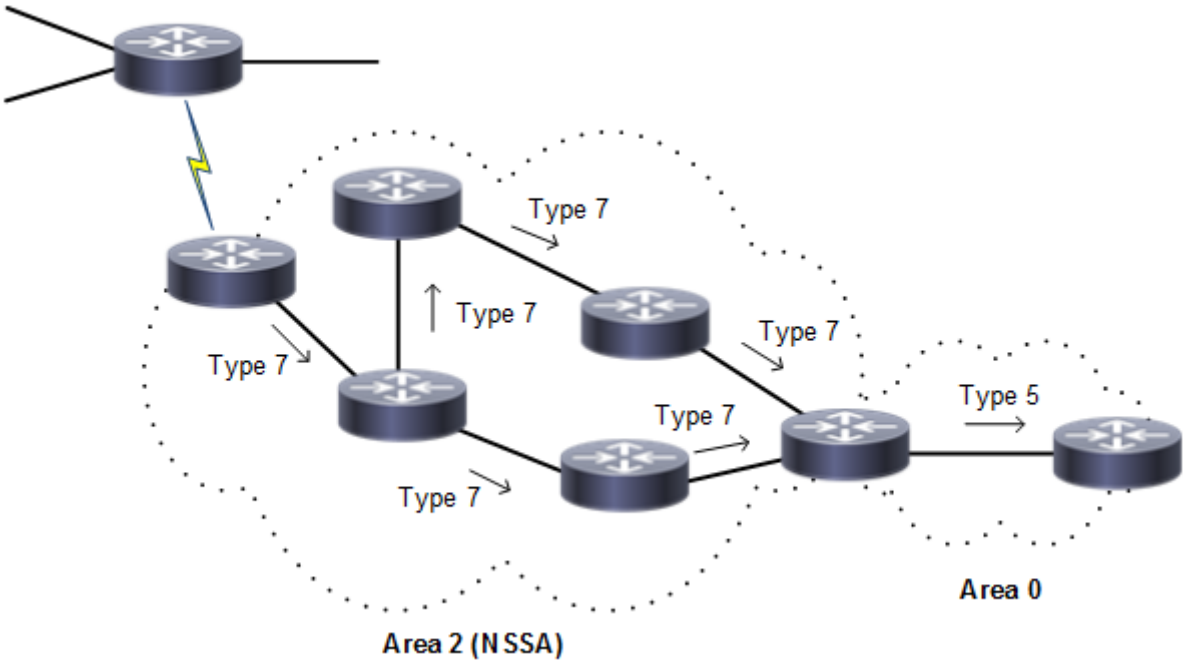


Figure 5-76: Translating Type 7 LSAs into Type 5 LSAs

NSSA with Route Options

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 5-77, 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

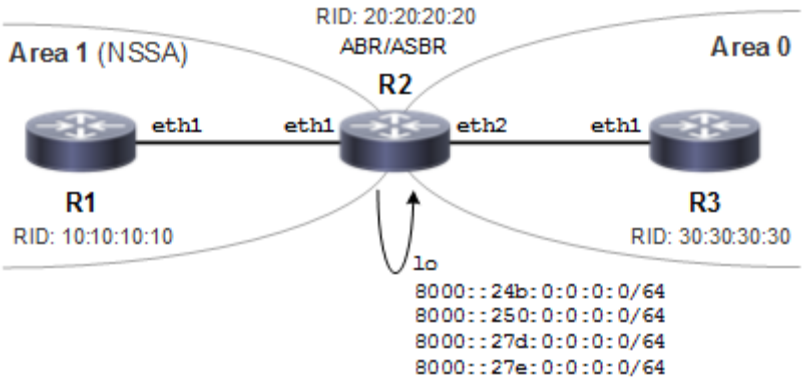


Figure 5-77: NSSA with Route Options

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    eth2       0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/Backup     00:00:38    eth1       0
```

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 5-78 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

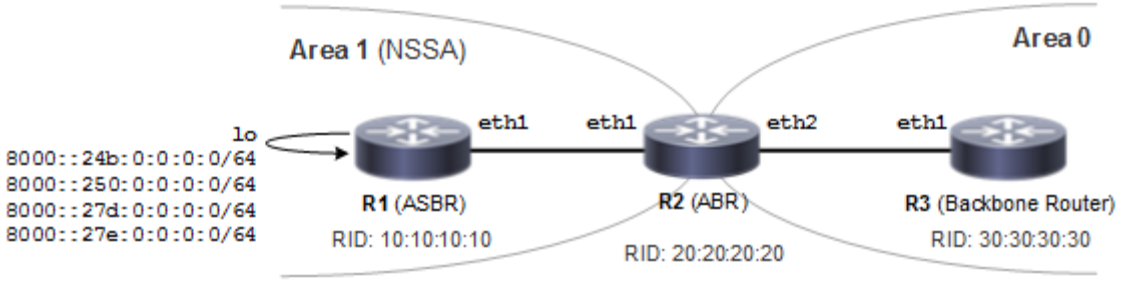


Figure 5-78: Using the summary-address Option

Configuration

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-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 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 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`	Configure the Router in 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 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 5-79:

- 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

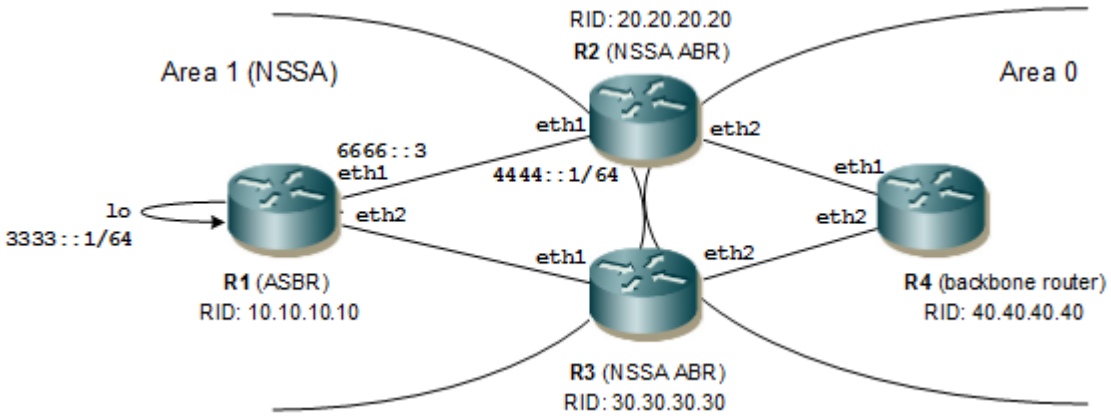


Figure 5-79: Using the translator-role Option

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

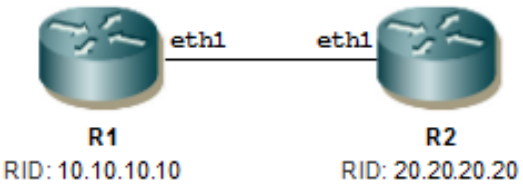


Figure 5-80: LSA Suppression

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 DUT 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.

```
DUT#sh ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                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)
```

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

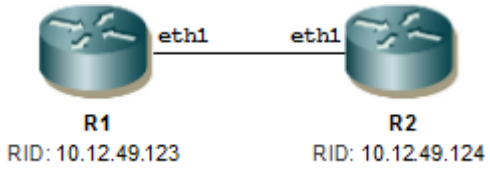


Figure 5-81: IPv4 Address Family on OSPFv3

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)#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)#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 5-82 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

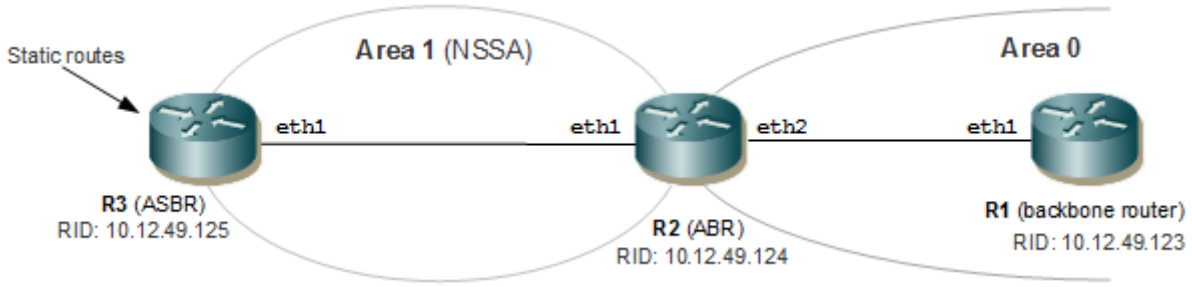


Figure 5-82: Originate Type-7 LSAs and Translate to Type-5 under Address Family IPv4

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 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)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.
`(config-router)#ip route 15.15.15.0/24 null`	Configure the static route with the nexthop address set to null
`(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)#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 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.

```
DUT#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           95
10.12.49.124      1   Full/Backup     00:00:38    eth2          94
```

Validation 2

Verify that the ABR has External LSA Type 5 in its Database.

Note: Check that R3 has generated a Type 7 LSA.

```
R3#sh ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.129) (Process 1)

                AS-external-LSA
```

```
LS age: 1517
LS Type: AS-External-LSA
Link State ID: 0.0.0.1
Advertising Router: 10.12.49.124
LS Seq Number: 0x80000003
Checksum: 0x597D
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 10.12.49.0/24
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 991
LS Type: AS-External-LSA
Link State ID: 0.0.0.11
Advertising Router: 10.12.49.124
LS Seq Number: 0x80000001
Checksum: 0x4C60
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 21
  Prefix: 33.33.33.0/29
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x376B
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.1/32
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.14
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x3B65
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.2/32
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
```

```
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.15
  Advertising Router: 10.12.49.129
  LS Seq Number: 0x80000001
  Checksum: 0x3F5F
  Length: 36
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 33.33.33.3/32
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0


  LS age: 442
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.16
  Advertising Router: 10.12.49.129
  LS Seq Number: 0x80000001
  Checksum: 0x4359
  Length: 36
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 33.33.33.4/32
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0
```

Validation 3

Verify that FIB of backbone router has External Route as “O E2”.

```
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

Gateway of last resort is 10.12.49.1 to network 0.0.0.0

K*      0.0.0.0/0 via 10.12.49.1, eth0
C       10.12.49.0/24 is directly connected, eth0
C       11.11.11.0/24 is directly connected, eth1
C       11.13.11.0/24 is directly connected, eth3
C       11.14.11.0/24 is directly connected, eth4
C       11.15.11.0/24 is directly connected, eth5
C       12.12.12.0/24 is directly connected, eth1
O IA    30.30.30.0/24 [110/2] via 12.12.12.12, eth1
O E2    33.33.33.0/29 [110/21] via 12.12.12.12, eth1
O E2    33.33.33.1/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.2/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.3/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.4/32 [110/20] via 12.12.12.12, eth1
C       127.0.0.0/8 is directly connected, lo
K       169.254.0.0/16 is directly connected, eth0
```

Summarize Intra-Area and External Routes

Figure 5-83 shows the configuration to enable intra-area and external route summarization. The IPv4 address family is enabled on R1. R2 summarizes the internal OSPF routes which R3 redistributes.

Topology

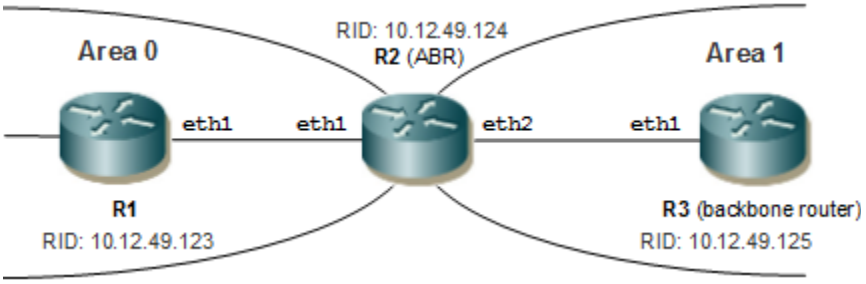


Figure 5-83: Enabling Intra-Area and External Route Summarization

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

`#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
`(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 10.10.10.2/24	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)#interface eth2	Enter interface mode
R2(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)#interface lo	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 101 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-router-af)#area 1 range 11.11.11.11/29 advertise	Summarize the internal OSPF routes.
(config-if)#exit	Exit interface mode

R3

#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)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
R3(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-router)#address-family ipv4 unicast	Enable the IPv4 address family
(config-router-af)#redistribute connected	Redistribute the connected route to generate external LSAs
(config-router-af)#summary-address 51.51.51.51/29	Summarize the external route at the ASBR.

Inter Area Route Aggregation Validation

Validation 1: Verify that adjacency has been established with the configured instance identifier.

```
DUT#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 aggregated OSPF IA route is available in FIB of R1.

```
R1#show ipv6 ospf n
OSPFv3 Process (100-ABC)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.12.49.124      1   Full/DR         00:00:32    eth1       64
```

Validation 3: Verify that the Inter-Area-Prefix-LSA has one prefix in the R1 Link State Database.

```
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, 00:06:54
C     10.12.49.123/32 is directly connected, lo, 00:06:54
O E2  10.12.49.125/32 [110/20] via 10.10.10.2, eth1, 00:05:58
O IA  20.20.20.0/24 [110/20] via 10.10.10.2, eth1, 00:06:04
C     127.0.0.0/8 is directly connected, lo, 00:06:58
C     192.168.20.0/24 is directly connected, eth0, 00:06:54

Gateway of last resort is not set


R1#show ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.123) (Process 100-ABC)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.12.49.123     787       0x80000001 0x1ed1      1
0.0.0.3         10.12.49.124     784       0x80000001 0x44a8      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.12.49.123     742       0x80000003 0x5610      1
0.0.0.0         10.12.49.124     739       0x80000003 0x5311      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.124     744       0x80000001 0x5763

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
```

```
0.0.0.1         10.12.49.124     779       0x80000002 0x5db9

                Inter-Area-Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.12.49.124     733       0x80000001 0x91e0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.12.49.124     738       0x80000001 0x0df7      2  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.123     738       0x80000003 0x8460
0.0.0.3         10.12.49.124     743       0x80000002 0xb231#show ipv6 ospf n
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
```

External Route Summarization Validation

Note: External route summarization is done at the ASBR.

Validation 1: Verify that single summarized external route in the ABR.

```
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     10.10.10.0/24 is directly connected, eth1, 00:06:40
C     10.12.49.124/32 is directly connected, lo, 00:06:40
O E2  10.12.49.125/32 [110/20] via 20.20.20.2, eth2, 00:05:48
C     20.20.20.0/24 is directly connected, eth2, 00:06:40
C     127.0.0.0/8 is directly connected, lo, 00:06:45
C     192.168.20.0/24 is directly connected, eth0, 00:06:40

Gateway of last resort is not set
```

Validation 2: Verify that a single Type 5 LSA is in the ABR's Link State Data Base.

```
R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.124) (Process 100-ABC)

                Link-LSA (Interface eth1)
```

```
    Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
    0.0.0.3         10.12.49.123     443       0x80000001 0x1ed1      1
    0.0.0.3         10.12.49.124     438       0x80000001 0x44a8      1

                    Link-LSA (Interface eth2)

    Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
    0.0.0.4         10.12.49.124     438       0x80000001 0xc2ee      1
    0.0.0.4         10.12.49.125     434       0x80000001 0xe8c5      1

                    Router-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum    Link
    0.0.0.0         10.12.49.123     398       0x80000003 0x5610      1
    0.0.0.0         10.12.49.124     393       0x80000003 0x5311      1

                    Network-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum
    0.0.0.3         10.12.49.124     398       0x80000001 0x5763

                    Inter-Area-Prefix-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum
    0.0.0.1         10.12.49.124     433       0x80000002 0x5db9

                    Inter-Area-Router-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum
    0.0.0.1         10.12.49.124     387       0x80000001 0x91e0

                    Intra-Area-Prefix-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
    0.0.0.2         10.12.49.124     392       0x80000001 0x0df7      2  Network-
    LSA

                    Intra-Area-Te-LSA (Area 0.0.0.0)

    Link State ID   ADV Router      Age       Seq#       CkSum
    0.0.0.3         10.12.49.123     393       0x80000003 0x8460
    0.0.0.3         10.12.49.124     398       0x80000002 0xb231

                    Router-LSA (Area 0.0.0.1)

    Link State ID   ADV Router      Age       Seq#       CkSum    Link
    0.0.0.0         10.12.49.124     393       0x80000004 0x87d8      1
    0.0.0.0         10.12.49.125     389       0x80000004 0x2a3d      1


                    AS-external-LSA

    Link State ID   ADV Router      Age       Seq#       CkSum   Route  Tag
    0.0.0.1         10.12.49.125     779       0x80000001 0x64f1 E2      0
    0.0.0.2         10.12.49.125     779       0x80000001 0xfba8 E2      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 5-84 shows the configuration to illustrate the distribute-list support for OSPFv3

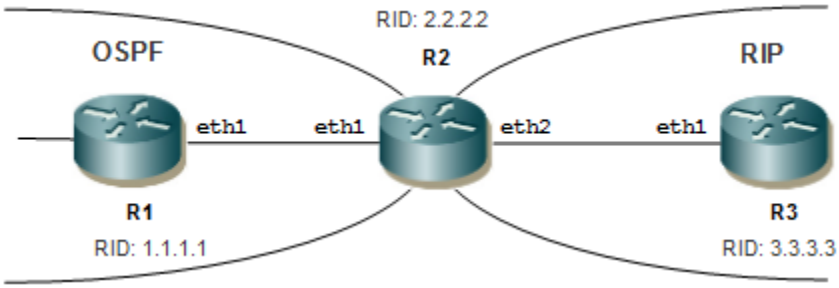


Figure 5-84: Basic Topology for Distribute-list

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)#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)#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)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID
`(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 eth1`	Configure RIP neighbor peer
`(config-router)#exit`	Exit router mode.
`(config)#ipv6 access-list 1 permit 7777::/64`	Configure access list to permit 7777::/64 and deny 8888::/64
`(config)#router ipv6 ospf proc1`	Configure the 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 the permitted routes
`(config-router)#exit`	Exit router mode
`(config)#ipv6 access-list 1`	Enter access-list mode
`(config-ipv6-acl)#permit ipv6 8888::1/64 any`	Configure access-list
`(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 eth2`	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 route 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
```

Loop Free Alternate

The diagram shows the configuration for the OSPFv3 Loop Free Alternate (LFA) feature.

Topology

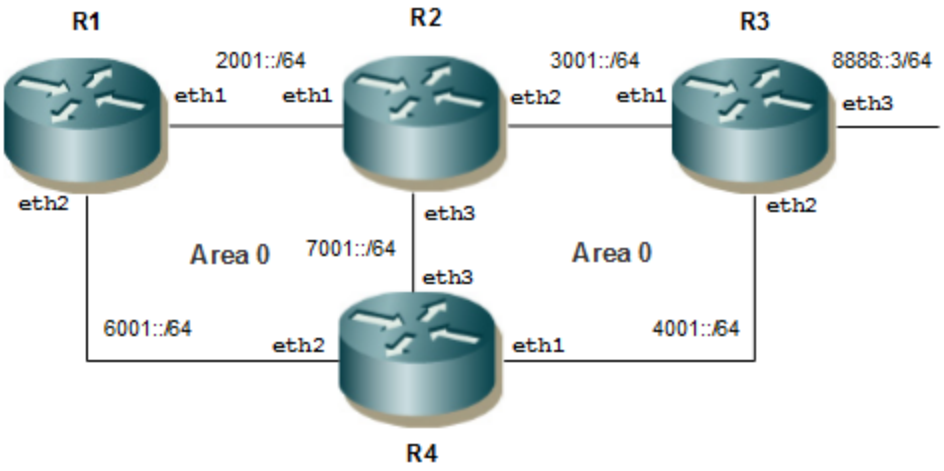


Figure 5-85: Basic OSPFv3 LFA Topology

Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 2001::1/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ipv6 address 6001::1/64`	Configure the IPv6address of the interface
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface
`(config-if)#ipv6 ospf cost 5`	Configure cost for the interface
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 ospf 1`	Configure the routing process and specify the Process ID (`1`).
`(config)#router-id 1.1.1.1`	Configure the router-id
`(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)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 2001::2/64`	Configure the IPv6 address of the interface

(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ipv6 address 3001::2/64	Configure the IPv6 address of the interface
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ipv6 address 7001::2/64	Configure the IP v6address of the interface
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#ipv6 ospf cost 2	Configure cost for the interface
(config)#router ipv6 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-id 2.2.2.2	Configure the router-id
(config-router)#end	Exit router mode

R3

#configure terminal	Enter configure mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 address 3001::3/64	Configure the IPv6 address of the interface
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ipv6 address 4001::3/64	Configure the IP v6address of the interface
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#ipv6 ospf cost 2	Configure cost for the interface
(config)#interface eth3	Enter interface mode
(config-if)#ipv6 address 8888::3/64	Configure the IP v6address of the interface
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface
(config-if)#exit	Exit interface mode
(config)#router ipv6 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-id 3.3.3.3	Configure the router-id
(config-router)#end	Exit router mode

R4

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 5001::4/64`	Configure the IPv6 address of the interface
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface
`(config-if)#ipv6 ospf cost 2`	Configure cost for the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ipv6 address 6001::4/64`	Configure the IPv6 address of the interface
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface
`(config-if)#ipv6 ospf cost 5`	Configure cost for the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth3`	Enter interface mode
`(config-if)#ipv6 address 7001::4/64`	Configure the IPv6 address of the interface
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface
`(config-if)#ipv6 ospf cost 2`	Configure cost for the interface
`(config)#router ipv6 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-id 4.4.4.4`	Configure the router-id
`(config-router)#end`	Exit router mode

Validation

Check OSPFv3 neighborship.

```
rtr1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:35    eth1       0
4.4.4.4           1   Full/DR         00:00:35    eth2       0
```

Check the OSPF route installation and LFA-FRR backup path for the primary path.

```
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, 1d18h11m
C      2001::/64 via ::, eth1, 01:33:09
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
```

```
O      4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C      5001::/64 via ::, eth3, 1d18h01m
C      6001::/64 via ::, eth2, 17:06:18
O      7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O      8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C      fe80::/64 via ::, eth2, 17:48:03
rtr1#show ipv6 route fast-reroute
IPv6 Fast-reroute Routing Table
Codes: R - RIP, O - OSPF,
       I - IS-IS, B - BGP
O      3001::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:59
O      4001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:09
O      7001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:59
O      8888::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:09
```

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)#interface eth2
(config-if)#ipv6 ospf fast-reroute per-prefix candidate disable
(config-if)#end
```

Verify that the `eth2` interface is not used for backup path calculation.

```
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, 1d18h11m
C      2001::/64 via ::, eth1, 01:33:09
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O      4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C      5001::/64 via ::, eth3, 1d18h01m
C      6001::/64 via ::, eth2, 17:06:18
O      7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O      8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C      fe80::/64 via ::, eth2, 17:48:03
rtr1#show ipv6 route fast-reroute
```

Now there is no LFA backup paths as we have disabled the interface from backup path calculation

Tie-Breaking Configuration:

By default, LFA backup path is calculated based on interface-disjoint. Other supported attributes are:

- Primary Path
- Broadcast-link protecting
- Node-protection

```
(config)#router ipv6 ospf 1
rtr1(config-router)#fast-reroute tie-break node-protecting index 1
```

Verify `show ipv6 route` and `show ipv6 route fast-reroute` for backup path calculated according to attributes configured above.

```
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, 1d18h15m
C      2001::/64 via ::, eth1, 01:37:43
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
O      4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
C      5001::/64 via ::, eth3, 1d18h06m
C      6001::/64 via ::, eth2, 17:10:52
O      7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
O      8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
C      fe80::/64 via ::, eth2, 17:52:37
rtr1#show ipv6 route fast-reroute
IPv6 Fast-reroute Routing Table
Codes: R - RIP, O - OSPF,
       I - IS-IS, B - BGP
O      4001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
O      7001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
O      8888::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
```

CHAPTER 6 BGP

This chapter contains basic Border Gateway Protocol configuration examples.

Enable BGP Routers in the Same Autonomous System

Figure 6-86 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

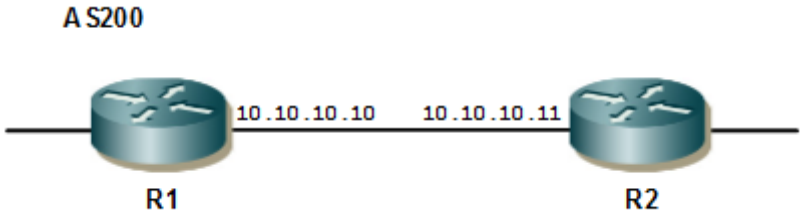


Figure 6-86: Routers in the Same Autonomous System

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

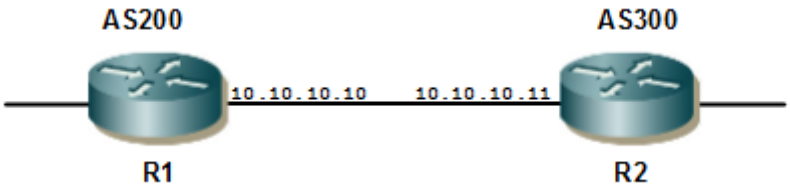


Figure 6-87: Routers in Different Autonomous Systems

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

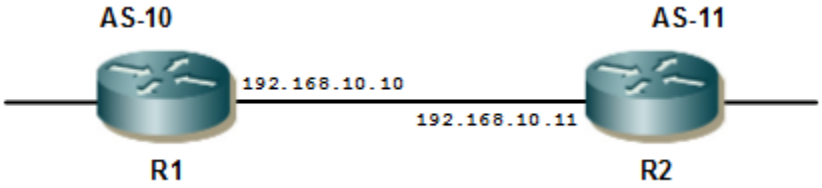


Figure 6-88: Configure Route-Map

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.

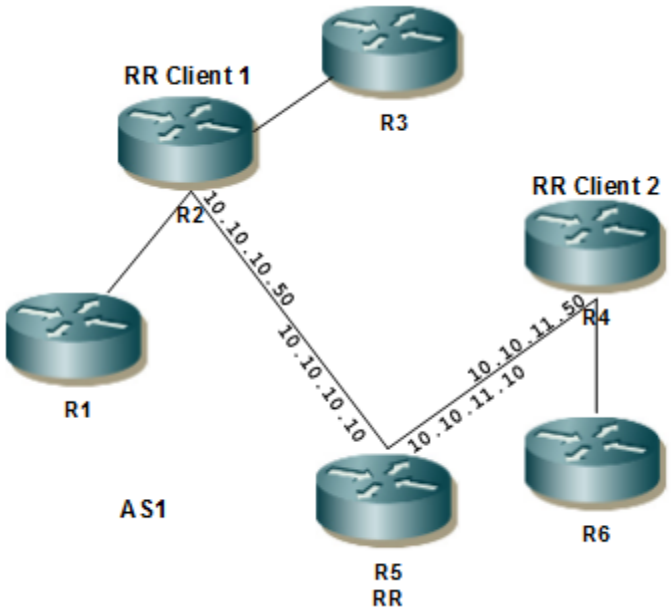


Figure 6-89: BGP Route Reflector

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

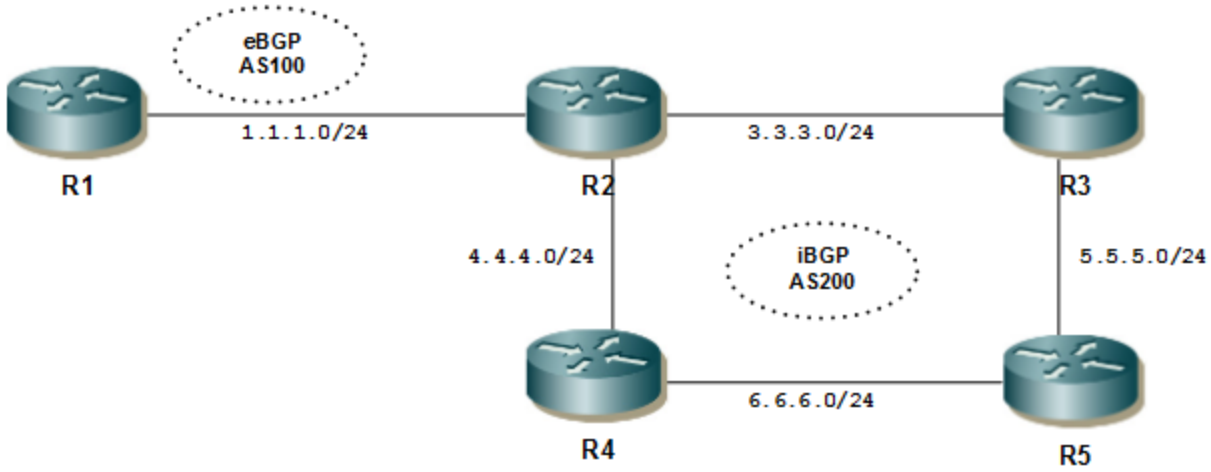


Figure 6-90: eBGP and iBGP Route Reflector Topology

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

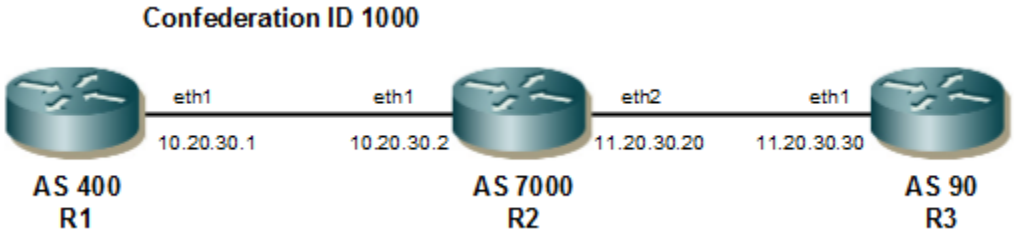


Figure 6-91: BGP Confederation

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.
`(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`).

`#configure terminal`	Enter configure mode.
`(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

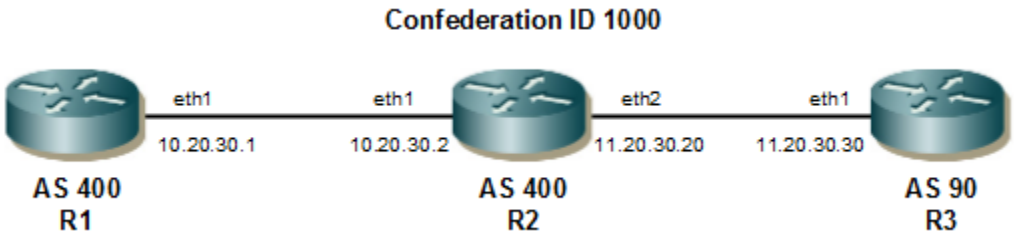


Figure 6-92: BGP Confederation with Multiple AS

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.

`#configure terminal`	Enter configure mode.
`(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

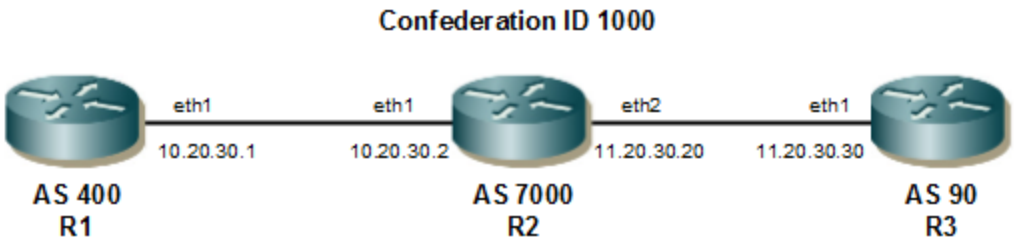


Figure 6-93: Single Confederation with Outside AS

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

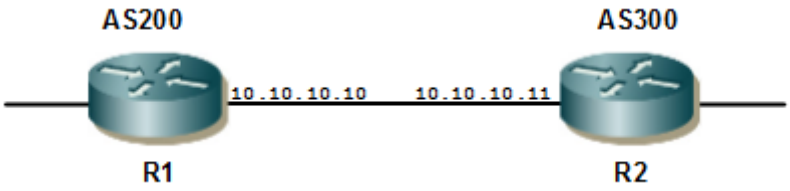


Figure 6-94: BGP Authentication

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.

`#configure terminal`	Enter configure mode.
`(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 10.10.10.11 password ABC`	Specify the password.

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 10.10.10.10 password ABC`	Specify the password.

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 6-95: 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.

#configure terminal	Enter configure mode.
(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)#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

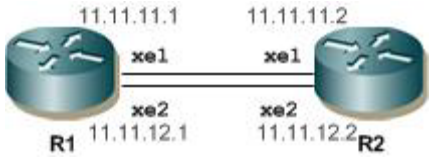


Figure 6-96: IPv4 VRF IBGP Peering

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

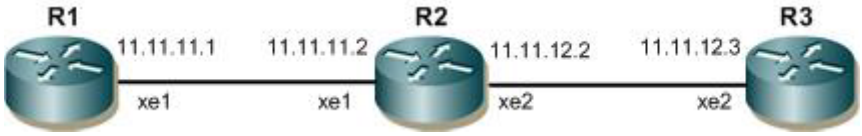


Figure 6-97: IPv4 EBGP Peering

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.

`#configure terminal`	Enter configure 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.
`(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.

#configure terminal	Enter configure 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.
(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

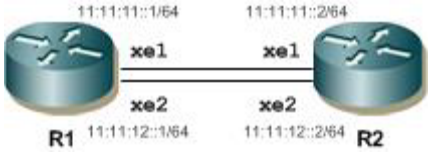


Figure 6-98: IPv6 IBGP Peering

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

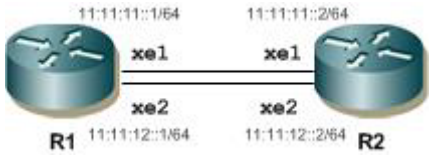


Figure 6-99: IPv6 VRF IBGP peering

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

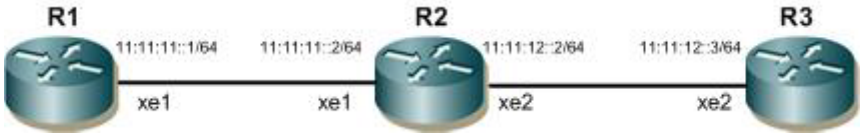


Figure 6-100: IPv6 EBGP peering

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

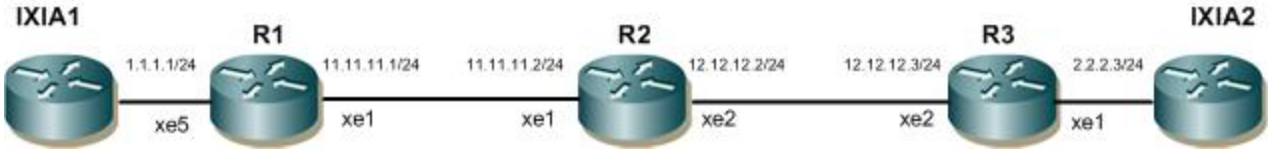


Figure 6-101: IPv4 IBGP VPNv4 Configuration

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-s lo	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

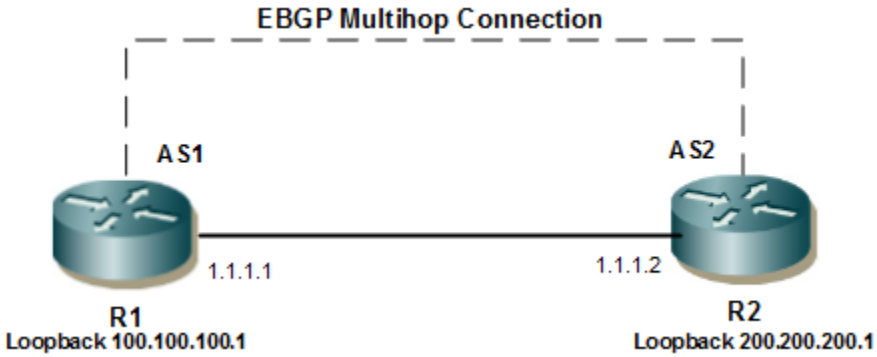


Figure 6-102: eBGP Multihop Connection

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.

In the following scenario, R1, R2, and R3 belong to the same peer group. R4 and R1 are eBGP peers. R1 is the route reflector (configuration not shown), and R2 and R3 are in AS 200. R4 is in AS 100.

Topology

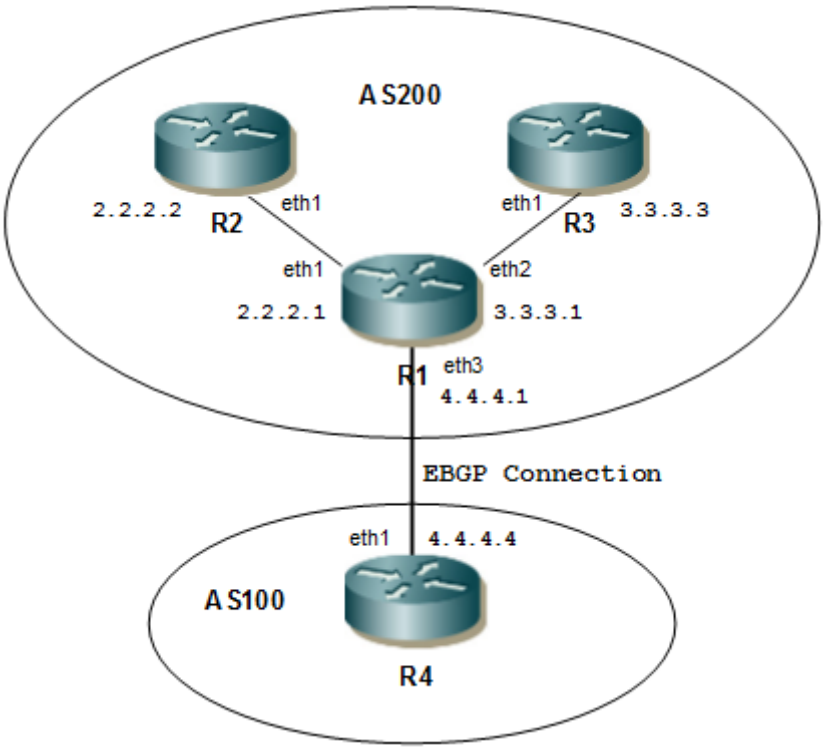


Figure 6-103: BGP Peer Groups

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 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)#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.

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
  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

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
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 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
  0 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
```

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

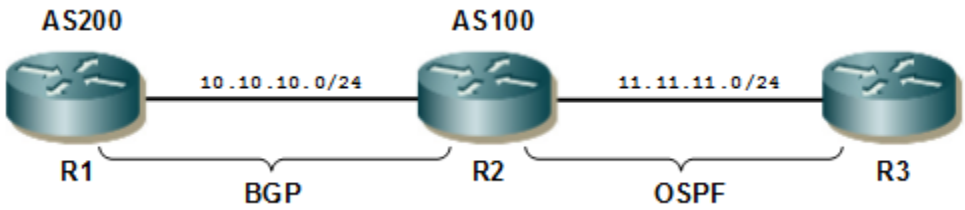


Figure 6-104: Redistribute with OSPF

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

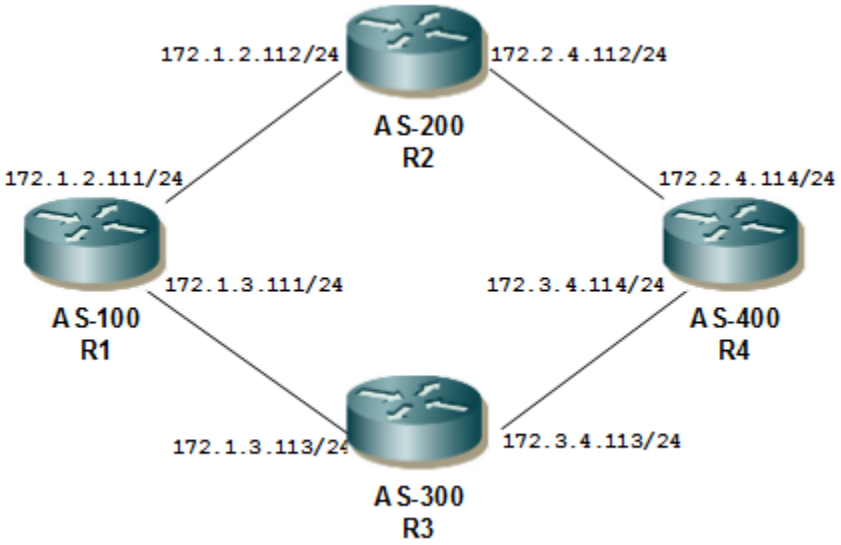


Figure 6-105: Multiple Instances of Same AS

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

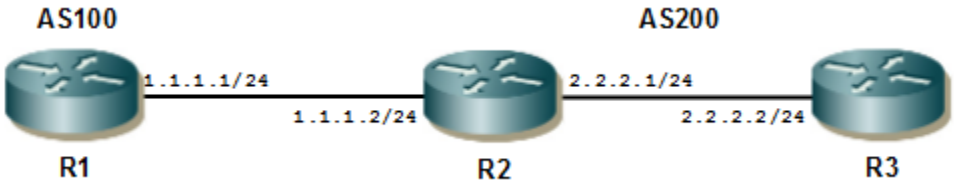


Figure 6-106: Remove MED Attribute

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 6-107: 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

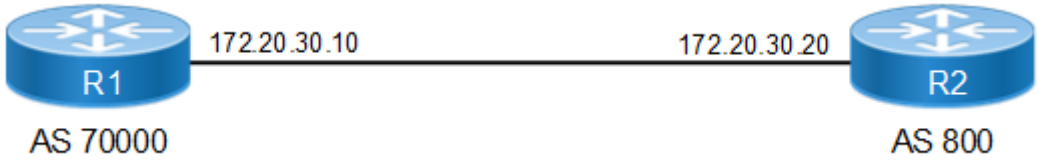


Figure 6-108: 4-Octet ASN on One Router

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

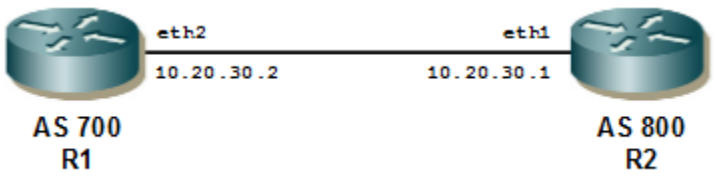


Figure 6-109: 4-Octet ASN

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

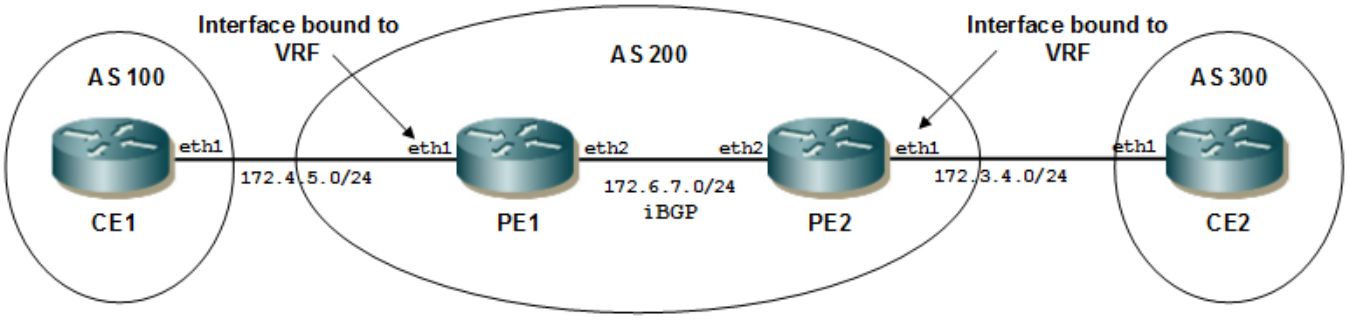


Figure 6-110: Extended Communities — 2-Byte ASN

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.

`#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-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.

`#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-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

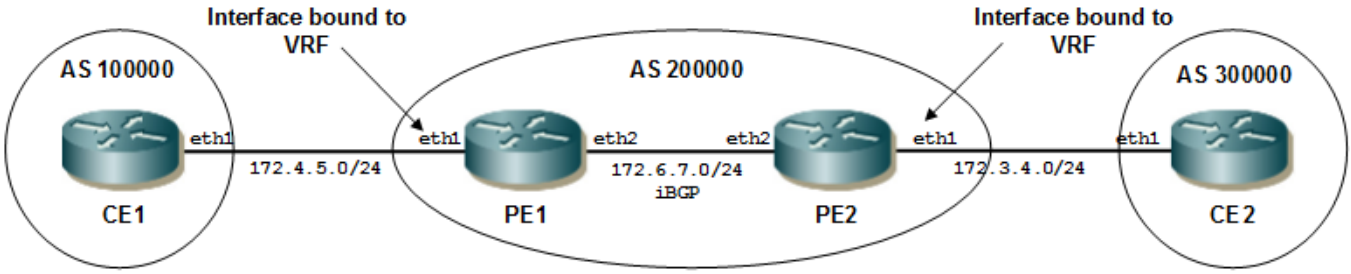


Figure 6-111: Extended Communities — 4-Byte ASN

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

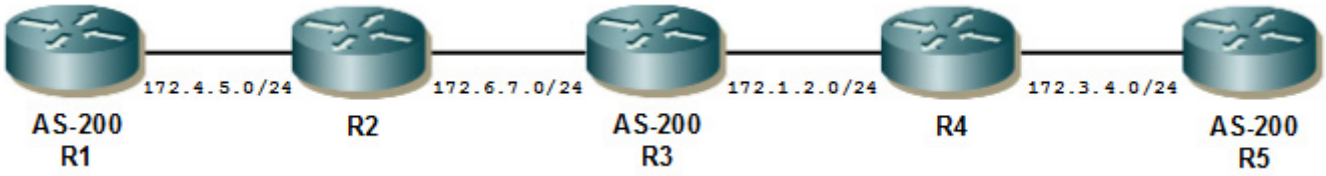


Figure 6-112: BGP Nexthop Tracking

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`).
`(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

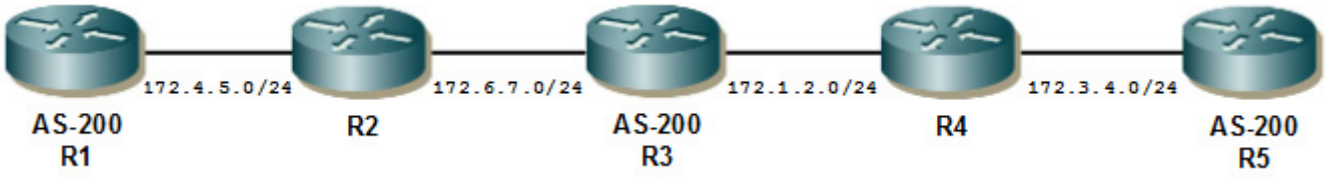


Figure 6-113: Topology for Nexthop Tracking Delay Timer

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.
`(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 Graceful Restart

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

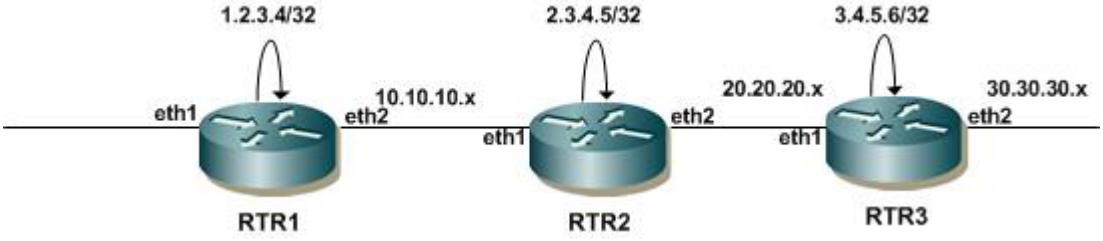


Figure 7: Device topology for BGP in VR/VRF

RTR1

`#configure terminal`	Enter Configuration mode
`(config)#interface lo`	Enter interface mode for loopback
`(config-if)#ip address 1.2.3.4/32 secondary`	Configure ip address on loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	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 1.2.3.4`	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 2.3.4.5/32 secondary`	Configure ip address on loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	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 eth2`	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 2.3.4.5`	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 3.4.5.6/32 secondary	Configure ip address on loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	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 3.4.5.6	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

```
#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    *>  1.2.3.4/32 is directly connected, lo, 00:10:23
```

```
B    *>  2.3.4.5/32 [20/0] via 10.10.10.2, xe52/1, 00:03:56
B    *>  3.4.5.6/32 [20/0] via 10.10.10.2, xe52/1, 00:00:56
C    *>  10.10.10.0/24 is directly connected, xe52/1, 00:09:37
B    *>  20.20.20.0/24 [20/0] via 10.10.10.2, xe52/1, 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    *>  1.2.3.4/32 [20/0] via 10.10.10.1, xe49/1, 00:03:52
C    *>  2.3.4.5/32 is directly connected, lo, 00:07:36
B    *>  3.4.5.6/32 [20/0] via 20.20.20.2, xe23, 00:00:57
C    *>  10.10.10.0/24 is directly connected, xe49/1, 00:07:12
C    *>  20.20.20.0/24 is directly connected, xe23, 00:06:31
C    *>  127.0.0.0/8 is directly connected, lo, 00:25:32

Gateway of last resort is not set
```

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    *> 1.2.3.4/32 [20/0] via 20.20.20.1, ge14, 00:01:15
B    *> 2.3.4.5/32 [20/0] via 20.20.20.1, ge14, 00:01:15
C    *> 3.4.5.6/32 is directly connected, lo
B    *> 10.10.10.0/24 [20/0] via 20.20.20.1, ge14, 00:01:15
C    *> 20.20.20.0/24 is directly connected, ge14
C    *> 127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

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 1.2.3.4/32 [20/0] via 10.10.10.1, xe49/1, 00:19:31
C    *>  2.3.4.5/32 is directly connected, lo, 00:50:45
B    *>p 3.4.5.6/32 [20/0] via 20.20.20.2, xe23, 00:19:32
C    *>  10.10.10.0/24 is directly connected, xe49/1, 00:50:21
C    *>  20.20.20.0/24 is directly connected, xe23, 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
     BGP        ACTIVE            57           2001/06/07 19:50:38
```

RTR1

```
#show ip bgp
BGP table version is 8, local router ID is 1.2.3.4
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
*>   1.2.3.4/32         0.0.0.0             0         100           32768    ?
```

```
S>    2.3.4.5/32          10.10.10.2           0          100           0        400 ?
S>    3.4.5.6/32          10.10.10.2           0          100           0        400 300 ?
*>    10.10.10.0/24       0.0.0.0              0          100           32768     ?
S                         10.10.10.2           0          100           0        400 ?
S>    20.20.20.0/24       10.10.10.2           0          100           0        400 ?

Total number of prefixes 5
```

RTR3

```
#sh ip bgp
BGP table version is 14, local router ID is 3.4.5.6
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
S>    1.2.3.4/32          20.20.20.1           0          100           0        400 100 ?
S>    2.3.4.5/32          20.20.20.1           0          100           0        400 ?
*>    3.4.5.6/32          0.0.0.0              0          100           32768     ?
S>    10.10.10.0/24       20.20.20.1           0          100           0        400 ?
*>    20.20.20.0/24       0.0.0.0              0          100           32768     ?
S                         20.20.20.1           0          100           0        400 ?

Total number of prefixes 5
```

BGP Distance

Administrative distance in BGP can be configured for a specific address family.

Topology

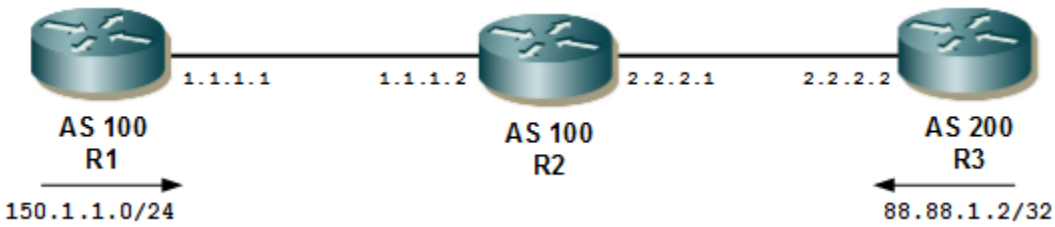


Figure 6-1: Administrative Distance for IPv4 BGP

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

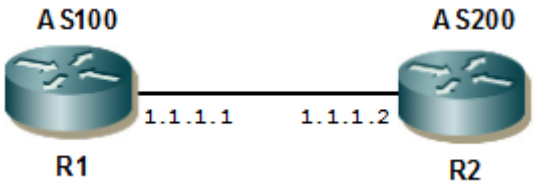


Figure 6-2: BGP Weight Per Peer

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 6-3, 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

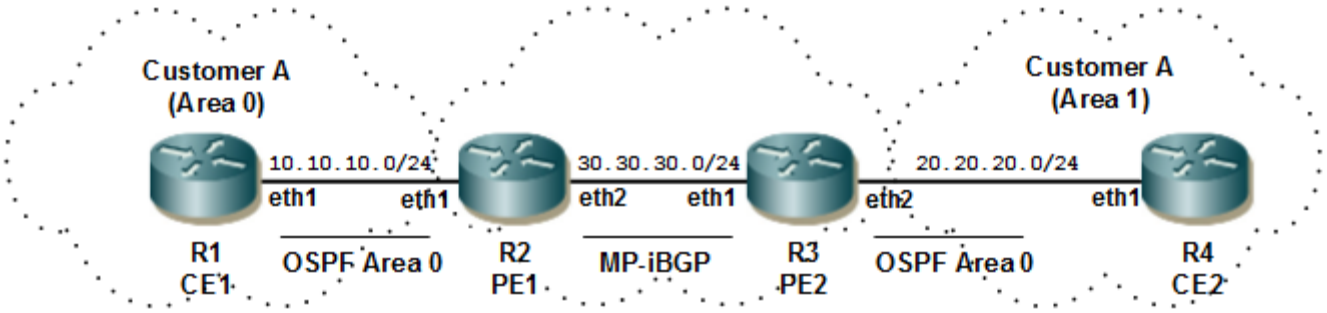


Figure 6-3: OSPF as PE-CE Protocol

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

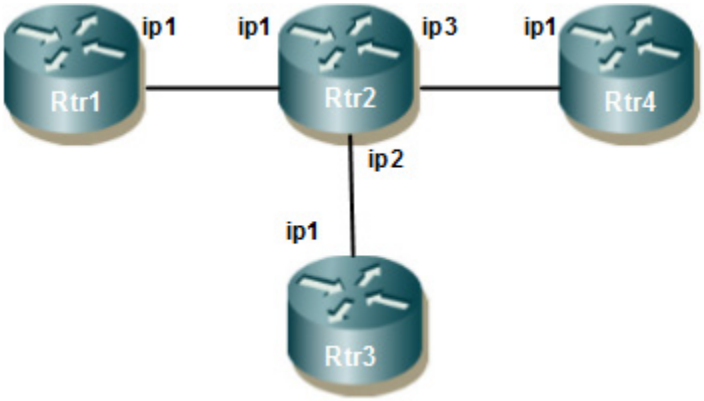


Figure 6-4: Multipath iBGP for IPv4

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

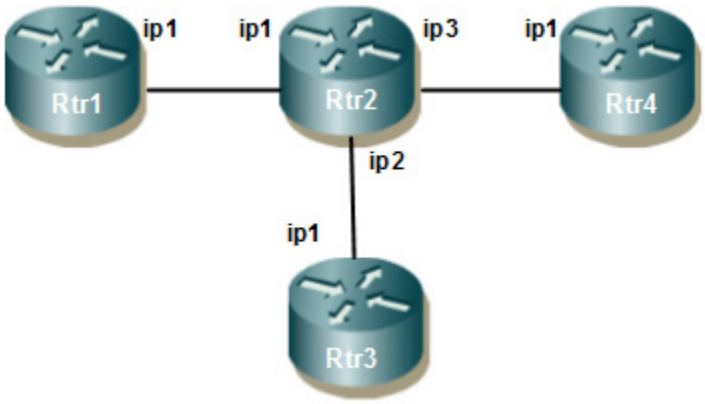


Figure 6-5: Multipath eBGP for IPv4

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.

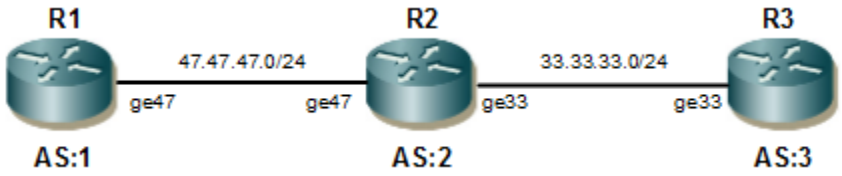


Figure 6-6: BGP AS-PATH Multipath-relax Topology

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 Graceful Shutdown

This section contains BGP graceful shutdown configuration examples.

BGP graceful shutdown reduces and avoid packets loss during maintenance shutdown by keeping the path undisturbed even after shutdown by lowering local preference so that routers of an AS can use this until they become aware of new path. If there is no alternate path available in the AS, the same path is used until forwarding failure occurs.

BGP graceful shutdown is supported for both BGP-IPv4 and BGP-IPv6 configurations.

BGP Graceful Shutdown on an Interface

Figure 6-7 shows the minimum configuration required to enable graceful shutdown on an interface. R1, R2, and R3 are three routers in three different ASs. R4 is another router in another AS forming an alternate path – R1 R4 R3 to the primary path.

Note: BGP graceful shutdown is only supported for eBGP configurations. It is not supported for iBGP configurations.

Topology

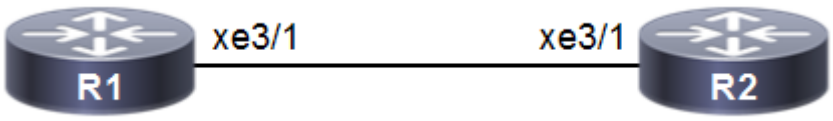


Figure 6-7: BGP Graceful Shutdown Topology 1

R1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.2 remote-as 200`	Establish eBGP neighborship with R2.

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 6.6.6.1/32 secondary`	Specify IP address.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.1 remote-as 100`	Establish eBGP neighborship with R1.
`(config-router)#bgp g-shut-capable`	Enable the graceful shutdown capability on the DUT.
`(config-router)#neighbor 10.10.10.1 g-shut`	Enable graceful shutdown functionality on the connected interface to R1.
`(config-router)#neighbor 10.10.10.1 g-shut-timer 70`	Configure the value of the graceful shutdown timer. After the timer expires, the BGP session initiated for graceful shutdown is shut down. The supported range for the graceful shutdown timer value is from 10 to 65535, in seconds. The default value is 60 seconds.
`(config-router)#network 6.6.6.1/32`	Specify the network to be advertised by the BGP routing process from DUT.

Validation

Checking for BGP Graceful Shutdown Community Tag on R1:

```
R1#show ip bgp 6.6.6.1
BGP routing table entry for 6.6.6.1/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  200
    10.10.10.2 from 10.10.10.2 (192.168.52.10)
      Origin IGP, metric 0, localpref 0, valid, external, best
      Community: 0:65535
      Last update: Fri May 10 07:42:14 2019

RTR1#
```

BGP Graceful Shutdown on a Router

Figure 6-8 shows the minimum configuration required to enable graceful shutdown at the router level. R1, R2, and R3 are three routers in three different ASs. R4 is another router in another AS forming an alternate path – R1 R4 R3 to the primary path.

Note: BGP graceful shutdown at the router level is used to bring down all the BGP sessions on the DUT. If there is still an alternate path for the data traffic, it takes that path.

Topology

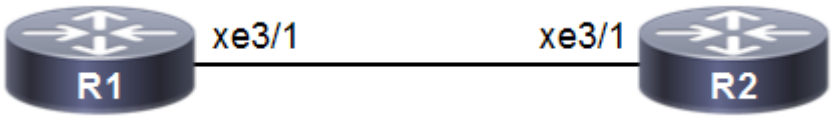


Figure 6-8: BGP Graceful Shutdown Topology 2

R1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.2 remote-as 200`	Establish eBGP neighborship with R2.

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 70.70.70.1/32 secondary`	Specify IP address.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.1 remote-as 100`	Establish eBGP neighborship with R1.
`(config-router)#bgp g-shut-capable`	Enabling the graceful shutdown capability on the DUT.
`(config-router)#bgp g-shut`	Enable BGP graceful shutdown functionality at the router level.
`(config-router)#bgp g-shut-local-preference 100`	Configure the local preference value of the routes to be used during graceful shutdown. This local preference is different from the BGP local preference value and is set in order to make the alternative path a preferred one in the case of graceful shutdown. The supported range of the local preference value is from 0 to 4294967295.
`(config-router)#network 7.7.7.1/32`	Specify the network to be advertised by the BGP routing process from DUT.

Validation

```
R1#show ip bgp 7.7.7.1
BGP routing table entry for 7.7.7.1/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  200
    10.10.10.2 from 10.10.10.2 (192.168.52.10)
      Origin IGP, metric 0, localpref 0, valid, external, best
      Community: 0:65535
      Last update: Fri May 10 07:56:56 2019
```

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

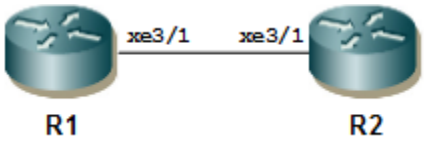


Figure 6-9: BFP FIB Install Topology

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.

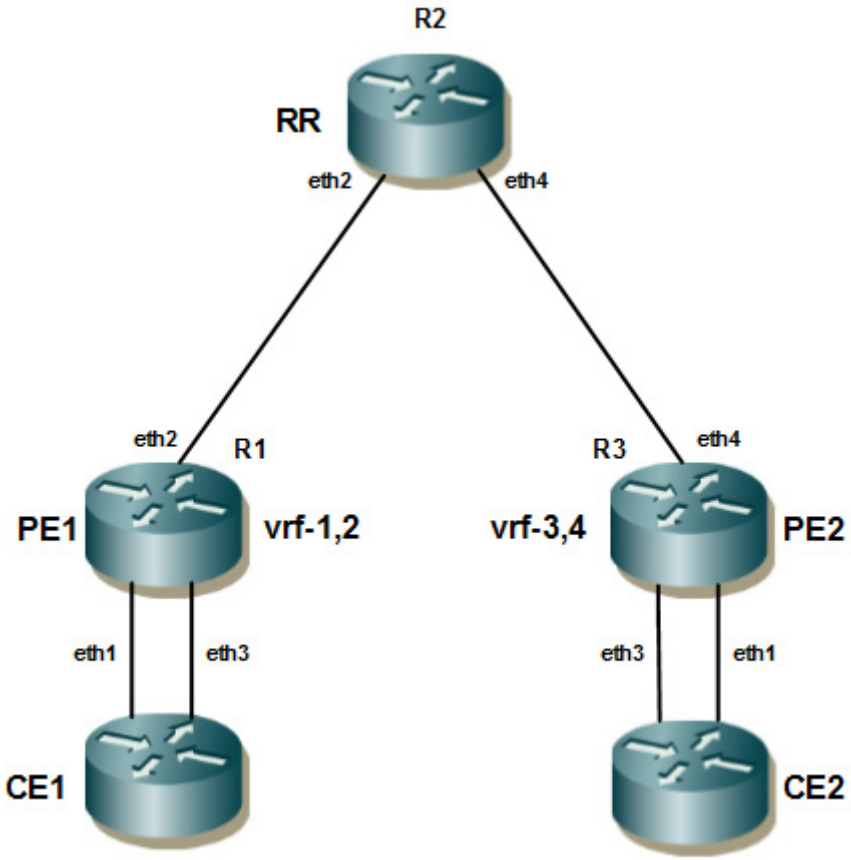


Figure 6-10: Route-target Filter Topology

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 Unnumbered

This chapter contains configurations for BGP unnumbered interface which provides BGP peering with minimal configuration.

Overview

BGP protocol is used to exchange IP prefixes between AS. For BGP neighbor ship to be established, IPv4 address configuration on peer is pre-requisite. In a large network, this can consume a lot of your address space, requiring a separate IP address for each peer-facing interface apart from administrator effort in configuration. When a BGP peer advertises an IPv4 prefix, it must include an IPv4 next hop address, which is usually the address of the advertising router; for this each BGP peer should have an IPv4 address. This feature is to enable BGP peering with minimal configuration, less IPv4 address-space.

For DC use-case, where hundreds of switches are connected in CLOS topology, configuring each neighbor is a time-taking. To minimize this, this feature will help in avoiding IP address configuration for BGP neighbor. Along with IP address, knowing the remote ASN number is not required for neighbor configuration.

Topology

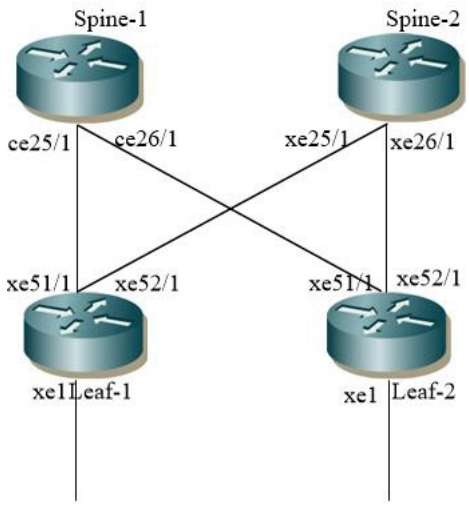


Figure 6-11: BGP-Unnumbered

Leaf1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback
`(config-if)#ip address 22.22.22.22/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit interface mode and return to Configure mode
`(config)#interface xe1`	Enter Interface mode for xe1.
`(config-if)#ip address 9.9.9.1/24`	Assign IP address on xe1 interface.
`config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe51/1`	Enter Interface mode for xe51/1.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe52/1`	Enter Interface mode for xe52/1.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 65500`	Enter into Router BGP mode
`(config-router)bgp router-id 100.100.100.1`	Assign BGP router ID
`(config-router)# network 22.22.22.22/32`	Specify the network to be advertised by the BGP routing process.
`(config-router)# max-paths ebgp 2`	Configure eBGP max-paths.
`(config-router)# redistribute static`	Configure static redistribution.
`(config-router)#neighbor xe51/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#neighbor xe52/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode
`(config)#ip route 55.1.1.0/24 9.9.9.2`	Configure static route.
`(config)#exit`	Exit from configuration mode.

Leaf2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit interface mode and return to Configure mode
`(config)#interface xe1`	Enter Interface mode for xe1.
`(config-if)#ip address 2.2.2.1/24`	Assign IP address on xe1 interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe51/1`	Enter Interface mode for xe51/1.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe52/1`	Enter Interface mode for xe52/1.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 65501`	Enter into Router BGP mode
`(config-router)bgp router-id 100.100.100.2`	Assign BGP router ID
`(config-router)# network 33.33.33.33/32`	Specify the network to be advertised by the BGP routing process.
`(config-router)# max-paths ebgp 2`	Configure eBGP max-paths.
`(config-router)# redistribute static`	Configure static redistribution.
`(config-router)#neighbor xe51/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#neighbor xe52/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode
`(config)#ip route 65.1.1.0/24 2.2.2.2`	Configure static route.
`(config)#exit`	Exit from configuration mode.

Spine1

`configure terminal`	Enter configure mode.
`(config)#interface ce25/1`	Enter interface mode for ce25/1
`(config-if)# no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)# ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface ce26/1`	Enter interface mode for ce26/1
`(config-if)# no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)# ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 64601`	Enter into Router BGP mode
`(config-router)# bgp router-id 111.111.111.111`	Assign BGP router ID
`(config-router)#neighbor ce25/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#neighbor ce26/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode.
`(config)#exit`	Exit from configuration mode.

Spine2

`#configure terminal`	Enter configure mode.
`(config)#interface xe25/1`	Enter interface mode for xe25/1
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe26/1`	Enter Interface mode for xe26/1.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#ipv6 nd ra-interval 4`	Assign interval between IPv6 Router Advertisements.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 64601`	Enter into Router BGP mode
`(config-router)bgp router-id 111.111.111.112`	Assign BGP router ID
`(config-router)#neighbor xe25/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external).
`(config-router)# neighbor xe26/1 remote-as external`	Specify the neighbor connected interface and the ASN value of the neighbor (external)
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode.
`(config)#exit`	Exit from configuration mode.

Validation

Leaf1:

```
#show running-config bgp
router bgp 65500
 bgp router-id 100.100.100.1
 network 22.22.22.22/32
 max-paths ebgp 2
 redistribute static
 neighbor xe52/1 remote-as external
 neighbor xe52/1 capability extended-nexthop-encoding
 neighbor xe51/1 remote-as external
 neighbor xe51/1 capability extended-nexthop-encoding
!
#show ip bgp summary
BGP router identifier 100.100.100.1, local AS number 65500
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries

Neighbor V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
fe80::218:23ff:feca:fa73 4 64601    7         8       8      0      0
00:01:35               2
fe80::8eea:1bff:fed1:c6a24 64601   21         25       8      0      0
00:02:34               2

Total number of neighbors 2

Total number of Established sessions 2


#show ip bgp neighbors xe51/1
BGP neighbor is fe80::8eea:1bff:fed1:c6a2, remote AS 64601, local AS 65500,
external link
  Peering on interface xe51/1
  BGP version 4, local router ID 100.100.100.1, remote router ID
111.111.111.111
  BGP state = Established, up for 00:04:05
  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 24 messages, 0 notifications, 0 in queue
  Sent 27 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 8, neighbor version 8
  Index 2, Offset 0, Mask 0x4
    Extended Next Hop Encoding: advertised and received
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  3 announced prefixes

 Connections established 2; dropped 1
```

```
Local host: fe80::218:23ff:fea6:96a5, Local port: 34279
Foreign host: fe80::8eea:1bff:fed1:c6a2, Foreign port: 179
Nexthop: 100.100.100.1
Nexthop global: fe80::218:23ff:fea6:96a5
Nexthop local: fe80::218:23ff:fea6:96a5
BGP connection: shared network
Last Reset: 00:04:10, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)


#show ip bgp neighbors xe52/1
BGP neighbor is fe80::218:23ff:feca:fa73, remote AS 64601, local AS 65500,
external link
  Peering on interface xe52/1
  BGP version 4, local router ID 100.100.100.1, remote router ID
111.111.111.112
  BGP state = Established, up for 00:03:15
  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 11 messages, 0 notifications, 0 in queue
  Sent 12 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 0, Offset 0, Mask 0x1
    Extended Next Hop Encoding: advertised and received
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  3 announced prefixes

 Connections established 1; dropped 0
Local host: fe80::218:23ff:fea6:96a5, Local port: 40482
Foreign host: fe80::218:23ff:feca:fa73, Foreign port: 179
Nexthop: 100.100.100.1
Nexthop global: fe80::218:23ff:fea6:96a5
Nexthop local: fe80::218:23ff:fea6:96a5
BGP connection: shared network


#show ip bgp
BGP table version is 8, local router ID is 100.100.100.1
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
*>   22.22.22.22/32   0.0.0.0              0         100           32768    i
*>   33.33.33.33/32   fe80::8eea:1bff:fed1:c6a2    0        100          0
64601 65501 i
*                    fe80::218:23ff:feca:fa73     0        100          0
64601 65501 i
*>   55.1.1.0/24      9.9.9.2              0         100           32768    ?
*>   65.1.1.0/24      fe80::218:23ff:feca:fa73     0        100          0
64601 65501 ?
```

```
*                    fe80::8eea:1bff:fed1:c6a2     0        100          0
64601 65501 ?

Total number of prefixes 4


#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     9.9.9.0/24 is directly connected, xe1, 00:08:29
C     22.22.22.22/32 is directly connected, lo, 00:14:22
B     33.33.33.33/32 [20/0] via fe80::8eea:1bff:fed1:c6a2, xe51/1, 00:08:52
               [20/0] via fe80::218:23ff:feca:fa73, xe52/1
S     55.1.1.0/24 [1/0] via 9.9.9.2, xe1, 00:14:22
B     65.1.1.0/24 [20/0] via fe80::8eea:1bff:fed1:c6a2, xe51/1, 00:07:47
           [20/0] via fe80::218:23ff:feca:fa73, xe52/1
C     127.0.0.0/8 is directly connected, lo, 00:18:10

Gateway of last resort is not set
```

Spine1:

```
#show running-config bgp
!
router bgp 64601
 bgp router-id 111.111.111.111
 neighbor ce25/1 remote-as external
 neighbor ce25/1 capability extended-nexthop-encoding
 neighbor ce26/1 remote-as external
 neighbor ce26/1 capability extended-nexthop-encoding
!
#show ip bgp summary
BGP router identifier 111.111.111.111, local AS number 64601
BGP table version is 9
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
fe80::218:23ff:fea6:96a5 4 65500   49         45       9      0      0
00:12:58               2
fe80::aa2b:b5ff:fe8e:13da4 65501   44         41       9      0      0
00:12:50               2

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors ce25/1
```

```
BGP neighbor is fe80::218:23ff:fea6:96a5, remote AS 65500, local AS 64601,
external link
  Peering on interface ce25/1
  BGP version 4, local router ID 111.111.111.111, remote router ID
100.100.100.1
  BGP state = Established, up for 00:13:23
  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 49 messages, 1 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 30 seconds
 For address family: IPv4 Unicast
  BGP table version 9, neighbor version 9
  Index 1, Offset 0, Mask 0x2
    Extended Next Hop Encoding: advertised and received
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
Local host: fe80::8eea:1bff:fed1:c6a2, Local port: 179
Foreign host: fe80::218:23ff:fea6:96a5, Foreign port: 34279
Nexthop: 111.111.111.111
Nexthop global: fe80::8eea:1bff:fed1:c6a2
Nexthop local: fe80::8eea:1bff:fed1:c6a2
BGP connection: shared network
Last Reset: 00:13:23, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)


#show ip bgp neighbors ce26/1
BGP neighbor is fe80::aa2b:b5ff:fe8e:13da, remote AS 65501, local AS 64601,
external link
  Peering on interface ce26/1
  BGP version 4, local router ID 111.111.111.111, remote router ID
100.100.100.2
  BGP state = Established, up for 00:13:19
  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 44 messages, 1 notifications, 0 in queue
  Sent 42 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 9, neighbor version 9
  Index 2, Offset 0, Mask 0x4
    Extended Next Hop Encoding: advertised and received
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
```

```
Local host: fe80::8eea:1bff:fed1:c6a2, Local port: 39569
Foreign host: fe80::aa2b:b5ff:fe8e:13da, Foreign port: 179
Nexthop: 111.111.111.111
Nexthop global: fe80::8eea:1bff:fed1:c6a2
Nexthop local: fe80::8eea:1bff:fed1:c6a2
BGP connection: shared network
Last Reset: 00:13:24, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)


#show ip bgp
BGP table version is 9, local router ID is 111.111.111.111
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   fe80::218:23ff:fea6:96a5    0        100          0
65500 i
*>   33.33.33.33/32   fe80::aa2b:b5ff:fe8e:13da    0        100          0
65501 i
*>   55.1.1.0/24      fe80::218:23ff:fea6:96a5    0        100          0
65500 ?
*>   65.1.1.0/24      fe80::aa2b:b5ff:fe8e:13da    0        100          0
65501 ?

Total number of prefixes 4
#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     22.22.22.22/32 [20/0] via fe80::218:23ff:fea6:96a5, ce25/1, 00:12:42
B     33.33.33.33/32 [20/0] via fe80::aa2b:b5ff:fe8e:13da, ce26/1, 00:12:34
B     55.1.1.0/24 [20/0] via fe80::218:23ff:fea6:96a5, ce25/1, 00:11:29
B     65.1.1.0/24 [20/0] via fe80::aa2b:b5ff:fe8e:13da, ce26/1, 00:11:20
C     127.0.0.0/8 is directly connected, lo, 00:23:09

Gateway of last resort is not set
```

CHAPTER 7 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 RIP, 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 7-12 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.

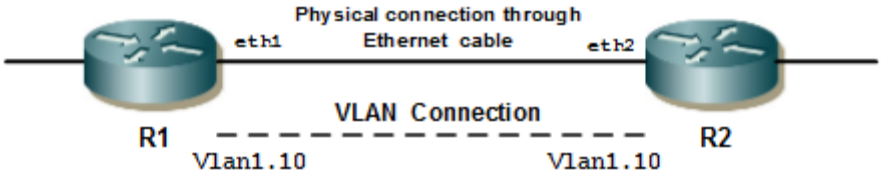


Figure 7-12: VLAN Connections

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 `eth1.1` 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 `eth1.10`. 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 8 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.

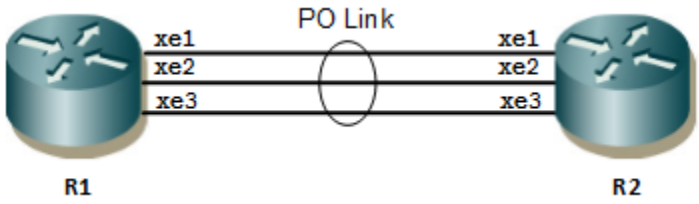


Figure 8-13: L3_LAG Topology

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
`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
`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
`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
`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
`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
`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
`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
`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
% 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
%  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

#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
```

VRF Lite Configuration Guide

Contents

This document contains these chapters and appendices:

CHAPTER 1 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 1-14: 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
`(config)#exit`	Exit configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate eth1 to vrf1.
`(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
```

CHAPTER 2 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 2-15: 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
Total number of full neighbors: 1
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, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:11:31

Gateway of last resort is not set
```

R2

```
#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State         Dead Time   Address       Interface          Instance
ID
2.2.2.1   1       Full/Backup      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, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:11:31
Gateway of last resort is not set
```

CHAPTER 3 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.

Note: This chapter covers BGP configuration in non-default VR and non-default VRF.

Topology

Figure 3-16: 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 100, local AS 200, external link
  BGP version 4, local router ID 2.2.2.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:00:14
  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 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 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: 179
Foreign host: 2.2.2.2, Foreign port: 36200
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
```

```
BGP connection: non shared network
```

Verify the routing table in R2

```
#show ip bgp neighbors
BBGP neighbor is 2.2.2.1, vrf vrf1, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 2.2.2.1
  BGP state = Established, up for 00:08:09
  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
  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 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: 36200
Foreign host: 2.2.2.1, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

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, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:20:40

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, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:14:53

Gateway of last resort is not set
```

CHAPTER 4 Inter-VRF Route Leaking Configuration

This chapter shows how to configure inter-VRF route leaking.

Overview

Virtual Routing and Forwarding (VRF) provides the ability to have multiple virtual routers on a single physical device. VRFs operate without knowledge of one another unless they are imported or exported into one another using inter-VRF route leaking. Inter-VRF route leaking allows leaking of route prefixes from one VRF instance to another VRF instance on the same physical router which eliminates the need for external routing.This is useful in cases where multiple VRFs share the same path to reach an external domain, while maintaining their internal routing information limited to their own VRF. This feature enables a data center to consolidate multiple VRF services onto a single server.

There are two types of inter-VRF route leaking:

- Static leaking: leaking manually configured static route entries from a source VRF to a global default VRF table.
- Dynamic leaking: leaking connected routes and dynamically learned routes from protocols such as ISIS, OSPF, and BGP from a source VRF to a destination VRF.

Static Leaking

Static route leaking directly between VRFs is not supported. What does work is routing traffic from a VRF to the global default VRF routing table. One advantage of using static route leaking is that you can configure exactly which routes are reachable without configuring BGP.

Topology

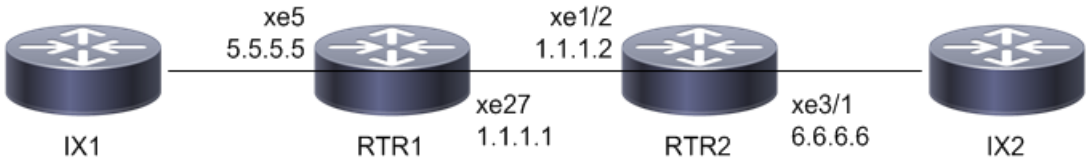


Figure 4-17: Static leaking

Configuration

The following steps describe how to configure static leaking.

RTR1

`RTR1#configure terminal`	Enter configure mode.
`RTR1(config)#interface xe5`	Enter interface mode
`RTR1(config-if)#ip address 5.5.5.5/24`	Assign IP address 5.5.5.5 to interface xe5
`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#interface xe27`	Enter interface mode

`RTR1(config-if)#ip address 1.1.1.1/24`	Assign IP address 1.1.1.1 to interface xe27
`RTR1(config-if)#exit`	Exit interface mode

RTR2

`RTR2#configure terminal`	Enter configure mode.
`RTR2(config)#interface xe1/2`	Enter interface mode
`RTR2(config-if)#ip address 1.1.1.2/24`	Assign IP address 1.1.1.2 to interface xe1/2
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#ip vrf vrf1`	Create VRF vrf1
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#interface xe3/1`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf1`	Associate xe3/1 to vrf1
`RTR2(config-if)#ip address 6.6.6.6/24`	Assign IP address 6.6.6.6 to interface xe3/1
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#ip route vrf vrf1 5.5.5.0/24 1.1.1.1 xe1/2 global`	Add static route to reach global default VRF table
`RTR2(config)#exit`	Exit configure mode

Validation

```
RTR2#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,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, xe1/2, 00:00:05
C     127.0.0.0/8 is directly connected, lo, 00:20:38
IP Route Table for VRF "management"
Gateway of last resort is 10.12.29.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 00:20:38
C     10.12.29.0/24 is directly connected, eth0, 00:20:38
C     127.0.0.0/8 is directly connected, lo.management, 00:20:38
IP Route Table for VRF "vrf1"
S    v5.5.5.0/24 [1/0] via 1.1.1.1, xe1/2, 00:05:20
C     6.6.6.0/24 is directly connected, xe3/1, 00:07:06
C     127.0.0.0/8 is directly connected, lo.vrf1, 00:12:25

RTR2#show ip route vrf all 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,
       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, xe1/2, 00:00:51
C    *>  127.0.0.0/8 is directly connected, lo, 00:21:24
IP Route Table for VRF "management"
S    *>  0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 00:21:24
C    *>  10.12.29.0/24 is directly connected, eth0, 00:21:24
C    *>  127.0.0.0/8 is directly connected, lo.management, 00:21:24
IP Route Table for VRF "vrf1"
S    *> v5.5.5.0/24 [1/0] via 1.1.1.1, xe1/2, 00:06:06
C    *>  6.6.6.0/24 is directly connected, xe3/1, 00:07:52
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 00:13:11
```

Dynamic Leaking

Route Leaking enables communication between isolated (virtual) routing domains by segregating and sharing a set of services that are available on one routing domain with other virtual domains. Inter-VRF route leaking enables a VRF to leak or export routes in its router to one or more VRFs. Dynamic route leaking enables a source VRF to share both its connected routes as well as dynamically learned routes from protocols such as ISIS, OSPF, and BGP to destination VRFs.

Topology

Figure 4-18: Dynamic leaking

Configuration

The following steps describe how to configure dynamic leaking.

RTR1

`RTR1#configure terminal`	Enter configure mode.
`RTR1(config)#interface xe5`	Enter interface mode
`RTR1(config-if)#ip address 5.5.5.5/24`	Assign IP address 5.5.5.5 to interface xe5
`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#interface xe27`	Enter interface mode
`RTR1(config-if)#ip address 1.1.1.1/24`	Assign IP address 1.1.1.1 to interface xe27

`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#router ospf 1`	Enter OSPF router mode
`RTR1(config-router)#network 1.1.1.0/24 area 0`	Specify the network type and area 0
`RTR1(config-router)#redistribute connected`	Redistribute connected route inside ospf
`RTR1(config-router)#exit`	Exit OSPF router mode

RTR2

`RTR2#configure terminal`	Enter configure mode.
`RTR2(config)#ip vrf vrf1`	Create VRF vrf1
`RTR2(config-vrf)#rd 100:1`	Configure route distinguisher in the VRF
`RTR2(config-vrf)#route-target export 100:1`	Configure export route target
`RTR2(config-vrf)#route-target import 200:1`	Configure import route target
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#ip vrf vrf2`	Create VRF vrf2
`RTR2(config-vrf)#rd 200:1`	Configure route distinguisher in the VRF
`RTR2(config-vrf)#route-target export 200:1`	Configure export route target
`RTR2(config-vrf)#route-target import 100:1`	Configure import route target
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#interface xe1/2`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf1`	Associate vrf1 to interface xe1/2
`RTR2(config-if)#ip address 1.1.1.2/24`	Assign IP address 1.1.1.2 to interface xe1/2
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#interface xe3/3`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf2`	Associate vrf2 to interface xe3/3
`RTR2(config-if)#ip address 2.2.2.2/24`	Assign IP address 2.2.2.2 to interface xe3/3
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#router ospf 1 vrf1`	Associate the OSPF process with vrf1
`RTR2(config-router)#network 1.1.1.0/24 area 0`	Specify the network type and area 0
`RTR2(config-router)#redistribute bgp`	Redistribute BGP routes inside OSPF
`RTR2(config-router)#exit`	Exit router mode
`RTR2(config)#router ospf 2 vrf2`	Associate the OSPF process with vrf2
`RTR2(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0
`RTR2(config-router)#redistribute bgp`	Redistribute BGP routes inside OSPF
`RTR2(config-router)#exit`	Exit router mode
`RTR2(config)#router bgp 100`	Enter BGP router mode
`RTR2(config-router)#address-family ipv4 vrf vrf1`	Enter address family mode for vrf1
`RTR2(config-router-af)#redistribute ospf 1`	Redistribute OSPF routes inside BGP
`RTR2(config-router-af)#exit-address-family`	Exit address family mode

`RTR2(config-router)#address-family ipv4 vrf vrf2`	Enter address family mode for vrf2
`RTR2(config-router-af)#redistribute ospf 2`	Redistribute OSPF routes inside BGP
`RTR2(config-router-af)#exit-address-family`	Exit address family mode
`RTR2(config-router)#exit`	Exit router mode

RTR3

`RTR3#configure terminal`	Enter configure mode.
`RTR3(config)#interface xe1`	Enter interface mode
`RTR3(config-if)#ip address 6.6.6.6/24`	Assign IP address 6.6.6.6 to interface xe1
`RTR3(config-if)#exit`	Exit from config mode
`RTR3(config)#interface xe33`	Enter interface mode
`RTR3(config-if)#ip address 2.2.2.3/24`	Assign IP address 2.2.2.3 to interface xe33
`RTR3(config-if)#exit`	Exit interface mode
`RTR3(config)#router ospf 2`	Enter OSPF router mode
`RTR3(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0
`RTR3(config-router)#redistribute connected`	Redistribute connected route inside ospf
`RTR3(config-router)#exit`	Exit OSPF router mode

Validation

RTR1

```
RTR1#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
1.1.1.2           1   Full/Backup     00:00:39    1.1.1.2         xe27

RTR1#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,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, xe27, 01:51:47
O E2  2.2.2.0/24 [110/1] via 1.1.1.2, xe27, 00:22:51
C     5.5.5.0/24 is directly connected, xe5, 02:16:39
O E2  6.6.6.0/24 [110/1] via 1.1.1.2, xe27, 00:22:51
```

```
C     127.0.0.0/8 is directly connected, lo, 02:25:23
```

RTR2

```
RTR2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
5.5.5.5           1   Full/DR         00:00:34    1.1.1.1         xe1/2                 0

Total number of full neighbors: 1
OSPF process 2 VRF(vrf2):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/DR         00:00:36    2.2.2.3         xe3/3                 0

RTR2#sh 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,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     127.0.0.0/8 is directly connected, lo, 02:06:03
IP Route Table for VRF "management"
Gateway of last resort is 10.12.29.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 02:06:03
C     10.12.29.0/24 is directly connected, eth0, 02:06:03
C     127.0.0.0/8 is directly connected, lo.management, 02:06:03
IP Route Table for VRF "vrf1"
C     1.1.1.0/24 is directly connected, xe1/2, 01:31:20
B    v2.2.2.0/24 [20/1] is directly connected, xe3/3, 00:02:35
O E2  5.5.5.0/24 [110/20] via 1.1.1.1, xe1/2, 00:07:12
B    v6.6.6.0/24 [20/20] via 2.2.2.3, xe3/3, 00:02:35
C     127.0.0.0/8 is directly connected, lo.vrf1, 01:40:49
IP Route Table for VRF "vrf2"
B    v1.1.1.0/24 [20/1] is directly connected, xe1/2, 00:03:35
C     2.2.2.0/24 is directly connected, xe3/3, 01:31:02
B    v5.5.5.0/24 [20/20] via 1.1.1.1, xe1/2, 00:03:35
O E2  6.6.6.0/24 [110/20] via 2.2.2.3, xe3/3, 00:06:52
C     127.0.0.0/8 is directly connected, lo.vrf2, 01:32:22

RTR2#sh ip route vrf all 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,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  127.0.0.0/8 is directly connected, lo, 02:07:34
IP Route Table for VRF "management"
S    *>  0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 02:07:34
C    *>  10.12.29.0/24 is directly connected, eth0, 02:07:34
C    *>  127.0.0.0/8 is directly connected, lo.management, 02:07:34
IP Route Table for VRF "vrf1"
C    *>  1.1.1.0/24 is directly connected, xe1/2, 01:32:51
O        1.1.1.0/24 [110/1] is directly connected, xe1/2, 00:09:13
B    *> v2.2.2.0/24 [20/1] is directly connected, xe3/3, 00:04:06
O E2 *>  5.5.5.0/24 [110/20] via 1.1.1.1, xe1/2, 00:08:43
B    *> v6.6.6.0/24 [20/20] via 2.2.2.3, xe3/3, 00:04:06
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:42:20
IP Route Table for VRF "vrf2"
B    *> v1.1.1.0/24 [20/1] is directly connected, xe1/2, 00:05:06
C    *>  2.2.2.0/24 is directly connected, xe3/3, 01:32:33
O        2.2.2.0/24 [110/1] is directly connected, xe3/3, 00:08:42
B    *> v5.5.5.0/24 [20/20] via 1.1.1.1, xe1/2, 00:05:06
O E2 *>  6.6.6.0/24 [110/20] via 2.2.2.3, xe3/3, 00:08:23
C    *>  127.0.0.0/8 is directly connected, lo.vrf2, 01:33:53
```

RTR3

```
RTR3#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/Backup     00:00:37    2.2.2.2         xe33                    0

RTR3#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,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O E2  1.1.1.0/24 [110/1] via 2.2.2.2, xe33, 00:20:12
C     2.2.2.0/24 is directly connected, xe33, 01:47:45
O E2  5.5.5.0/24 [110/1] via 2.2.2.2, xe33, 00:20:12
C     6.6.6.0/24 is directly connected, xe1, 02:00:13
C     127.0.0.0/8 is directly connected, lo, 02:21:14
```

Fundamental Layer 3 Command Reference

Contents

This document contains this chapter:

CHAPTER 1 Fundamental Layer 3 Commands

This chapter describes the fundamental Layer 3 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
(config)#
```

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 *
```

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`.

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)#
```

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 kernel
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 kernel
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
undebug rib kernel
```

Parameters

`all`	All debugging functions
`events`	Events
`packet`	Packet events
`recv`	Received packets
`send`	Sent packets

`detail`	Detailed information
`nsm`	NSM events
`kernel`	RIB kernel
`monitor`	Enable Monitor route netlink
`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 1-93 show the behavior of routes when `ribd` stops.

Table 1-93: 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 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
`global`	Global table lookup (to support inter-VRF static route leaking)
`<1-255>`	Administrative distance
`IFNAME`	Gateway nexthop interface name
`description`	Description of the static route maximum 80 character
`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 configured

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and was updated in OcNOS version 1.3.4.

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 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 user-defined 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, no user-defined VRFs exist, only the default VRF.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#
```

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
```

router-id

Use this command to add a router identifier for this system.

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

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 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
```

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
#
```

Table 1-94 explains the output fields.

Table 1-94: show ip 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 1-94: show ip 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	IP 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 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 1-95 explains the output fields.

Table 1-95: 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 1-95: 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 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

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 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 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
```

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
```

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:

- enable db-summary-opt
- fast-reroute keep-all-paths
- fast-reroute tie-break
- host area
- ip ospf authentication
- ip ospf authentication-key
- ip ospf bfd
- ip ospf cost
- ip ospf database-filter
- ip ospf dead-interval
- ip ospf disable
- ip ospf fast-reroute per-prefix candidate disable
- ip ospf flood-reduction
- ip ospf hello-interval
- ip ospf multi-area
- ip ospf message-digest-key
- ip ospf mtu
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- log-adjacency-changes
- max-concurrent-dd
- maximum-area
- neighbor
- network
- ospf abr-type
- ospf flood-reduction
- ospf restart helper
- ospf router-id
- overflow database
- overflow database external
- passive-interface
- redistribute
- restart ospf graceful
- router ospf
- show debugging ospf
- show ip ospf

- show ip ospf border-routers
- show ip ospf database brief
- 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)|
  stabilityinterval < 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)|
  stabilityinterval < 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.

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 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

`graceful`	Specify enabling OSPF graceful restart feature.

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
```

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 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
```

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
```

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 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.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. 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) index <1-10>
no fast-reroute tie-break
no fast-reroute tie-break (primary-path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint) index <1-10>
```

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`

Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.

`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.

`index` Tie break priority. A lower value has higher preference.

`<1-10>` Range of priority values.

Defaults

By default, LFA backup path is calculated based on interface-disjoint.

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

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 (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.
`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 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

`grace-period`	Specify the grace period.
`<1-1800>`	Specify the grace 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 {only-reload|only-upgrade|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

`only-reload`	Help only on software reloads.
`only-upgrade`	Help only on software upgrades.
`max-grace-period`	Help only if received grace-period is less than this value.
`<1-1800>`	Help only if received grace-period is less than this value.
`never`	Prevent the neighbor from entering helper mode.
`router-id`	Neighbor to never to act as helper.
`A.B.C.D`	Router ID of neighbor to never to act as helper.
`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)#ospf restart helper only-reload

#configure terminal
(config)#ospf restart helper only-reload max-grace-period 200

#configure terminal
(config)#no ospf restart helper never router-id all
```

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
```

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

`grace-period`	Specify a grace period.
`<1-1800>`	Specify a 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
```

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 1-96 explains the routing process fields.

Table 1-96: 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 1-96: 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 1-96: 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 1-97 explains the border router fields.

Table 1-97: 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 1-98 explains the fields for each database entry.

Table 1-98: 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 1-99 explains the fields for each database entry.

Table 1-99: 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 1-100.
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 1-99: 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 1-100 explains the fields for each database entry.

Table 1-100: 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 1-100: 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 1-101 explains the fields for each database entry.

Table 1-101: 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 1-102 explains the fields for each database entry.

Table 1-102: 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 1-103 explains the fields for each database entry.

Table 1-103: 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 1-104 explains the fields for each database entry.

Table 1-104: 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 1-105 explains the fields for each database entry.

Table 1-105: 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 1-106 explains the fields in the output.

Table 1-106: 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 1-107 explains the fields in the output.

Table 1-107: 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 1-108 explains the fields for each interface entry.

Table 1-108: 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 1-108: 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 1-109 explains the fields for each adjacency entry.

Table 1-109: 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 1-109: 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 1-110 explains the fields for each neighbor entry.

Table 1-110: OSPF neighbor output details

Field	Description
OSPF process	OSPF process identifier.
Neighbor ID	OSPF router identifier of the neighbor.

Table 1-110: 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 1-111 explains the fields for each neighbor detail entry.

Table 1-111: 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 1-110.
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 1-100.
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 1-111: 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 1-112 explains the fields of route codes.

Table 1-112: 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 1-113 shows the route entry fields.

Table 1-113: route entry output details

Field	Description
Codes	As explained in Table 1-112.
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 1-114 explains the fields for each virtual-links entry.

Table 1-114: 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 1-115 explains the fields for each ip protocol entry.

Table 1-115: 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 1-115: 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 OSPFv3 Commands

This chapter provides an alphabetized reference for each of the OSPFv3 commands. It includes the following commands:

- ipv6 ospf mtu-ignore
- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf restart grace-period
- ipv6 ospf restart helper
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- ipv6 te-metric
- max-concurrent-dd
- passive-interface
- redistribute
- restart ipv6 ospf graceful
- 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.

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.

- `<0-4294967295>`

  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
```

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
```

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 lfa

Use this command to specify the debugging options for OSPFv3 Loop-free Alternate path

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf lfa
no debug ipv6 ospf lfa
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf lfa
```

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
```

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
```

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPFv3 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 ipv6 ospf 200
(config-router)#fast-reroute keep-all-paths
```

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.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. 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) index <1-4>
no fast-reroute tie-break (primary-path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint) index <1-4>
no fast-reroute tie-break
```

Parameters

`primary-path`	When there are multiple loop-free alternate paths. The primary path is selected for an frr if it is node-protecting as well as link-protecting
`interface-disjoint`	Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.
`node-protecting`	Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.
`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.
`index`	Tie break priority. A lower value has higher preference.
`<1-4>`	Range of priority values.

Defaults

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 200
(config-router)#fast-reroute tie-break interface-disjoint index 1
```

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-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 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

`grace-period`	Specify the grace period.
`<1-1800>`	Specify the 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 {only-reload|only-upgrade|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 {only-reload|only-upgrade|max-grace-period|never
  router-id (A.B.C.D|all)}
```

Parameters

`only-reload`	Help only on software reloads.
`only-upgrade`	Help only on software upgrades.
`max-grace-period`	
	Help only if received grace-period is less than this value.
`<1-1800>`	Help only if received grace-period is less than this value.
`never`	Prevent the neighbor from entering helper mode.
`router-id`	Router of neighbor to never to act as helper.
`A.B.C.D`	Router ID of neighbor 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)#ipv6 ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#ipv6 ospf restart helper only-reload

#configure terminal
(config)#ipv6 ospf restart helper only-reload max-grace-period 200

#configure terminal
```

```
(config)#no ipv6 ospf restart helper never
```

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
```

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

`grace-period`	Specify a grace period.
`<1-1800>`	Specify a 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
```

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 2-116 explains the fields for each ospf entry.

Table 2-116: 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 2-117 explains the fields for each database entry.

Table 2-117: 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 2-117: 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 2-118 explains the fields for each ospf interface entry.

Table 2-118: 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: • Ethernet is Broadcast • Serial p2p non-broadcast • 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 2-119 explains the fields for each ospf neighbor entry.

Table 2-119: 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.
Dead timer due in	The countdown timer for marking neighbor connections dead. In this example, the Deat Timer has been deactivated.

Table 2-119: show ipv6 ospf neighbor output details (Continued)

Field	Description
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 2-120 explains the fields for each ospf route entry.

Table 2-120: 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 2-121 explains the fields for each ospfv3 topology entry.

Table 2-121: show ipv6 ospfv3 topology output details

Field	Description
OSPFv3 path to Area	Area ID in IPv4 format.
Router ID	ID in IPv4 format,

Table 2-121: 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 2-122 explains the fields for each ospf virtual-links entry.

Table 2-122: 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 2-123 explains the fields.

Table 2-123: 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 3 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)#
```

Routing Information Protocol Command Reference

Contents

This document contains these chapters and appendix:

CHAPTER 1 Routing Information Protocol Commands

This chapter provides an alphabetized reference for each of the Routing Information Protocol (RIP) commands, which support IPv4. It includes the following commands:

- show ip rip
- show ip rip interface
- show ip rip statistics
- snmp restart rip
- timers basic
- version

accept-lifetime

Use this command to specify the time period during which the authentication key on a key chain is received as valid.

Use the `no` option with this command to disable it.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

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 (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the time when accept-lifetime expires in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to expire.
`MONTH`	Specify the month of the year to expire (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to expire.
`duration`	Specify the duration of the key in seconds <1-2147483646>.
`infinite`	Specify the end time to never expire.

Default

None

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

(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#no accept-lifetime
```

cisco-metric-behavior

Use this command to enable the metric update consistent with Cisco.

Use either the `no` or `disable` parameter with this command to disable this feature.

Command Syntax

```
cisco-metric-behavior (enable|disable)
no cisco-metric-behavior
```

Parameters

`enable`	Enable updating the metric consistent with Cisco.
`disable`	Disable updating the metric consistent with Cisco.

Default

By default, the Cisco metric-behavior is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable the metric update behavior to be consistent with Cisco in the Router mode.

```
#configure terminal
(config)#router rip
 (config-router)#cisco-metric-behavior enable
```

clear ip rip route

Use this command to clear specific data from the RIP routing tables.

Using this command with the `all` parameter, clears the RIP table of all the routes. If you do not want that your RIP network to be deleted, use the `redistribute connected` command and make the RIP network a connected route. To delete the RIP routes learned from neighbor and also keep the RIP network intact, use the `rip` (`clear ip rip route rip`) parameter with this command.

Command Syntax

```
clear ip rip route (A.B.C.D/M|rip|kernel|connected|static|ospf|isis|bgp|all)
```

Parameters

`A.B.C.D/M`	Removes entries which exactly match this destination address from RIP routing table.
`bgp`	Removes only BGP routes from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`isis`	Removes only IS-IS routes from the RIP routing table
`kernel`	Removes kernel entries from the RIP routing table.
`ospf`	Removes only OSPF routes from the RIP routing table.
`rip`	Removes only RIP routes from the RIP routing table.
`static`	Removes static entries from the RIP routing table.
`all`	Removes the entire RIP routing table.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip rip route 10.0.0.0/8
#clear ip rip route ospf
```

clear ip rip route vrf NAME

Use this command to clear all IPv4 RIP VRF route or any specific prefix RIP VRF route of any particular VRF name.

Command Syntax

```
clear ip rip route vrf NAME (*|A.B.C.D/M)
```

Parameters

A.B.C.D/M	Removes entries with the prefix specified.
*	Removes all routes
NAME	VPN Routing or Forwarding instance name

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip rip route vrf myVRF *
```

clear ip rip statistics

Use this command to clear an IPv4 RIP statistics.

Command Syntax

```
clear ip rip statistics (IFNAME |)
```

Parameters

IFNAME	Removes entries from the interface.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip rip statistics
```

debug rip

Use this command to specify the options for the displayed debugging information for RIP events, RIP packets and RIP NSM.

Use the `no` parameter with this command to disable all debugging. The `undebug` alias command can also be used.

Command Syntax

```
debug rip (all|)
debug rip bfd
debug rip events
debug rip nsm
debug rip packet (recv|send|) (detail|)
debug rip rib
no debug rip (all|)
no debug rip bfd
no debug rip events
no debug rip nsm
no debug rip packet (recv|send|) (detail|)
no debug rip rib
undebug rip (all|)
undebug rip bfd
undebug rip events
undebug rip nsm
undebug rip packet (recv|send|) (detail|)
undebug rip rib
```

Parameters

`all`	Debug all RIP information.
`bfd`	Debug all RIP and BFD information.
`events`	Debug RIP events.
`nsm`	Debug RIP and NSM communications.
`packet`	Debug RIP packets, only
`recv`	Debug received packets.
`rib`	Debug RIP and RIB communications.
`send`	Debug sent packets.
`detail`	Display detailed information for the sent or received packet.

Default

Disabled

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example specifies the options for the displayed debugging information in `Configure` mode prompt.

```
#configure terminal
(config)#debug rip events
(config)#debug rip packet send detail
(config)#debug rip nsm
```

The following example shows to disable all debugging in `Privileged Exec` mode prompt.

```
#undebug rip events
#undebug rip packet send detail
#undebug rip nsm
```

default-information originate

Use this command to add default routes to the RIP updates.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
default-information originate (always|) (route-map WORD|)
no default-information originate
```

Parameters

`always`	Always advertise default route
`route map`	Route map reference
`WORD`	Pointer to route-map entries

Default

Disabled

Command Mode*

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#default-information originate route-map pmap
```

default-metric

Use this command to specify the metrics to be assigned to redistributed routers.

This command is used in conjunction with the `redistribute` command to make the routing protocol use the specified metric value for all redistributed routes. A default metric is useful in redistributing routes with incompatible metrics. Every protocol has different metrics and can not be compared directly. Default metric provides the standard to compare. All routes that are redistributed will use the default metric.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
default-metric <1-15>
no default-metric
```

Parameter

`<1-15>`	Default metric.

Default

By default, the metric value is set to 1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example assigns the cost of 10 to the OSPF routes which are redistributed into RIP.

```
#configure terminal
(config)#router rip
(config-router)#redistribute ospf
(config-router)#default-metric 10
```

distance

Use this command to set the administrative distance. The administrative distance is a feature used by the routers to select the path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicating a more reliable protocol.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
distance <1-255>
distance <1-255> A.B.C.D/M (WORD|)
no distance (<1-255>|)
no distance <1-255> A.B.C.D/M (WORD|)
```

Parameters

`<1-255>`	Specify the administrative distance value.
`A.B.C.D./M`	Specify the network prefix and length
`WORD`	Specify the access list name.

Default

By default, the administrative distance is 120.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#distance 8 10.0.0.0/8 mylist
```

distribute-list

Use this command to filter incoming or outgoing route updates using an access list or a prefix list. You can filter out incoming or outgoing route updates using an access list or a prefix list. If you do not specify the name of the interface, the filter will be applied to all the interfaces.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
distribute-list WORD (in|out) (IFNAME|)
distribute-list prefix WORD (in|out) (IFNAME|)
no distribute-list WORD (in|out) (IFNAME|)
no distribute-list prefix WORD (in|out) (IFNAME|)
```

Parameters

`WORD`	Specify the IPv4 access-list number or name to use.
`prefix`	Filter prefixes in routing updates.
`WORD`	Specify the name of the IPv4 prefix-list to use.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`IFNAME`	Specify the name of the interface on which distribute-list applies.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rip
(config-router)#distribute-list prefix myfilter in eth0
```

ip rip authentication key-chain

Use this command to enable RIPv2 authentication on an interface and specify the name of the key chain to be used. If you do not configure a key chain results in no authentication.

Use the `no` parameter with this command to disable this function.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax

```
ip rip authentication key-chain LINE
no ip rip authentication key-chain (LINE|)
```

Parameters

`LINE`	Specify the name of the key chain.

Default

If you do not configure a key chain, authentication is not used.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, interface eth0 is configured key-chain authentication and the name is specified as `mykey`. This name is used to enter the key-chain mode to specify the password. See the key command.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip authentication key-chain mykey
```

ip rip authentication mode

Use this command to specify the type of authentication mode used for RIP v2 packets.

Use the `no` parameter with this command to restore clear text authentication.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax

```
ip rip authentication mode md5
ip rip authentication mode text
no ip rip authentication mode
```

Parameters

`md5`	Uses the keyed MD5 authentication algorithm.
`text`	Specify the clear text or simple password authentication.

Default

No authentication mode is enabled by default. But, when any authentication key (string or key-chain) is configured, text authentication mode is enabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows `md5` authentication configured on the `eth1` interface, ensuring authentication of RIP packets received.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip authentication mode md5
```

ip rip authentication string

Use this command to specify the authentication string or password used by a key.

You can configure authentication for a single key or multiple keys at different times. Use this command to specify password for a single key on an interface.

Use the `no` parameter with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for how this command is related to the other authentication commands.

Command Syntax

```
ip rip authentication string LINE
no ip rip authentication string
```

Parameters

`LINE`	Specify the authentication string or password used by a key.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, the interface `eth1` is configured to have an authentication string as `guest`, any receiving RIP packet in that interface should have the same string as password.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip authentication string guest
```

ip rip receive-packet

Use this command to configure the interface to enable the reception of RIP packets.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
ip rip receive-packet
no ip rip receive-packet
```

Parameters

None

Default

Receive-packet is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows packet receiving being turned on for interface `eth0`.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip receive-packet
```

ip rip receive version

Use this command to receive specified version of RIP packets on an interface basis using version control, and override the setting of the version command.

Use the `no` form of this command to use the setting established by the version command.

Command Syntax

```
ip rip receive version (1|2)
ip rip receive version 1 2
ip rip receive version 2 1
no ip rip receive version
```

Parameters

`1`	Specify acceptance of RIP version 1 packets on the interface.
`2`	Specify acceptance of RIP version 2 packets on the interface.
`1 2`	Specify acceptance of RIP version 1 and version 2 packets on the interface.
`2 1`	Specify acceptance of RIP version 2 and version 1 packets on the interface.

Default

Version 2

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, interface eth1 in configured to receive both RIP version 1 and 2 packets.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip receive version 1 2
```

ip rip send-packet

Use this command to enable sending RIP packets through the current interface.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
ip rip send-packet
no ip rip send-packet
```

Parameters

None

Default

Send packet is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows packet sending being turned on for interface `eth0`.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip send-packet
```

ip rip send version

Use this command to send RIP packets on an interface using version control. In addition to version 1 and version 2, compatible version packets can be specified. With the parameter 1-compatible, a version 2 RIP interface will broadcast the packets instead of multicasting them.

This command applies to a specific interface and overrides any the version specified by the `version` command.

Use the `no` parameter with this command to use the global RIP version control rules.

Command Syntax

```
ip rip send version (1|2|1-compatible)
ip rip send version 1 2
ip rip send version 2 1
no ip rip send version
```

Parameters

`1`	Specify sending RIP version 1 packets out of an interface.
`2`	Specify sending RIP version 2 packets out of an interface.
`1 2`	Specify acceptance of RIP version 1 and version 2 packets on the interface.
`2 1`	Specify acceptance of RIP version 2 and version 1 packets on the interface.
`1-compatible`	Specify sending RIP version 1 compatible packets from a version 2 RIP interface.

Default

Version 2

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, interface eth1 is configured to send both RIP version 1 and 2 packets.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip send version 1 2
```

ip rip split-horizon

Use this command to perform the split-horizon action on the interface

This command helps avoid including routes in updates sent to the same gateway from which they were learned. Using the `split horizon` command omits routes learned from one neighbor, in updates sent to that neighbor. Using the `poisoned` parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
ip rip split-horizon
ip rip split-horizon poisoned
no ip rip split-horizon
```

Parameter

`poisoned`	Performs split-horizon with poisoned reverse.

Default

Split horizon poisoned

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip split-horizon poisoned
```

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.

Use the no option with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax

```
key <0-2147483647>
no key <0-2147483647>
```

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, RIP 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

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
```

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.

Use the no option with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax

```
key chain WORD
no key chain WORD
```

Parameter

`WORD`	Specify the name of the key chain to manage.

Default

None

Command Mode

Configure mode and Keychain 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 into `keychain` mode prompt.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

The following example shows the creation of a key chain named `mykeychain3` in the Keychain mode and the addition of an authentication key `key10` in the same mode.

```
(config-keychain)#key chain mykeychain3
(config-keychain)#key 10
(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.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

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

Disabled

Command Mode

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
```

maximum-prefix

Use this command to configure the maximum prefix.

Use the `no` parameter with this command to disable the limiting of the number of RIP routes in the routing table.

Command Syntax

```
maximum-prefix <1-65535> (<1-100>|)
no maximum-prefix
```

Parameters

`<1-65535>`	The maximum number of RIP routes allowed.
`<1-100>`	Percentage of maximum routes to generate a warning. The default threshold is 75%.

Default

The default maximum-prefix threshold is 75%.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#maximum-prefix 150
```

neighbor

Use this command to specify a neighbor router. It is used for each connected point-to-point link. This command to exchanges non-broadcast routing information. It can be used multiple times for additional neighbors.

`Passive-interface` command disables sending routing updates on an interface. Use the `neighbor` command in conjunction with the `passive-interface` command to send routing updates to specific neighbors.

Use the `no` parameter with this command to disable the specific router.

Command Syntax

```
neighbor A.B.C.D
no neighbor A.B.C.D
```

Parameter

`A.B.C.D`	An IP address of a neighboring router with which the routing information will be exchanged.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#neighbor 10.7.1.12
```

network

Use this command to specify a network as one that runs RIP. This command specifies the networks to which routing updates will be sent and received. If a network is not specified, the interfaces in that network will not be advertised in any RIP update.

Use the `no` parameter with this command to remove the specified network as one that runs RIP.

Command Syntax

```
network A.B.C.D/M
network IFNAME
no network A.B.C.D/M
no network IFNAME
```

Parameters

`A.B.C.D/M`	The IP address prefix and length of this IP network.
`IFNAME`	Alphanumeric string that defines the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#network 10.0.0.0/8
(config-router)#network eth0
```

offset-list

Use this command to add an offset to in and out metrics to routes learned through RIP. This command specifies the offset value that is added to the routing metric. When the networks match the access list the offset is applied to the metrics. No change occurs if the offset value is zero.

Use the `no` parameter with this command to remove the offset list.

Command Syntax

```
offset-list WORD (in|out) <0-16> (IFNAME|)
no offset-list WORD (in|out) <0-16> (IFNAME|)
```

Parameters

`WORD`	Specify the access-list number or names to apply.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
`<0-16>`	Specify that the offset is used for metrics of networks matching the access list.
`IFNAME`	An alphanumeric string that specifies the interface to match.

Default

The default `offset value` is the interface metric value which is defined by the operating system.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In this example the router examines the RIP updates being sent out from interface eth0 and adds 16 hops to the routes matching the ip addresses specified in the access list `accesslist1`.

```
#configure terminal
(config)#router rip
(config-router)#offset-list accesslist1 in 16 eth0
```

passive-interface

Use this command to block RIP broadcast on the interface.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

Parameters

`IFNAME`	Specify the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#passive-interface eth0
```

recv-buffer-size

Use this command to run-time configure the RIP UDP receive-buffer size.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
recv-buffer-size <8192-2147483647>
no recv-buffer-size
```

Parameters

`<8192-2147483647>`

Specify the RIP UDP receive buffer size value.

Default

The default value of the RIP UDP receive-buffer size is 32768.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#recv-buffer-size 150000
```

redistribute

Use this command to redistribute information from other routing protocols.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|ospf|isis|bgp)
redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>
redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD
redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD
no redistribute (kernel|connected|static|ospf|isis|bgp)
no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>
no redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD
no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map
  WORD
```

Parameters

`bgp`	Redistribute from BGP routes
`connected`	Redistribute from connected routes
`isis`	Redistribute from ISO IS-IS routes
`kernel`	Redistribute from kernel routes
`ospf`	Redistribute from OSPFv3 routes
`static`	Redistribute from static routes
`metric`	Metric value
`<0-16>`	Specify a metric value
`route-map`	Route map reference
`WORD`	Specify name of the route-map

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#redistribute kernel
```

```
#configure terminal
(config)#router rip
(config-router)#redistribute kernel route-map myroutemap
```

route

Use this command to configure static RIP routes.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
route A.B.C.D/M
no route A.B.C.D/M
```

Parameter

`A.B.C.D/M`	Specify the IP address prefix and length.

Default

No route is added.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Use this command to add a static RIP route. This command is used most often for debugging purposes and does not show up in the kernel routing table. After adding the RIP route, it can be checked in the RIP routing table.

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#neighbor 10.10.10.10
(config-router)#route 10.10.10.0/24

(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#no route 10.10.10.0/24
```

router rip

Use this global command to enable a RIP routing process.

Use the `no` parameter with this command to disable RIP routing.

Command Syntax

```
router rip
no router rip
```

Parameter

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This command is used to begin the RIP routing process.

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#neighbor 10.10.10.10
```

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 send-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 (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the time when send-lifetime expires in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to expire.
`MONTH`	Specify the month of the year to expire (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to expire.
`duration`	Specify the duration of the key in seconds <1-2147483646>.
`infinite`	Specify the end time to never expire.

Default

Disabled

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 debugging rip

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging and RIP nsm debugging.

Command Syntax

```
show debugging rip
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging rip
R2#show debugging rip
RIP debugging status:
  RIP event debugging is on
  RIP packet detail debugging is on
  RIP RIB debugging is on
  RIP NSM debugging is on
  RIP BFD debugging is on

R2#
```

show ip protocols rip

Use this command to display RIP process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols rip
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is an example of the output from the `show ip protocols rip` command:

```
#show ip protocols rip
Routing Protocol is "rip"
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)
#
```

Figure 1-124 Explains the show command output details.

Table 1-124: Show ip protocols output details

Field	Description
Routing Protocol is "rip"	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.
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 rip

Use this command to show RIP routes.

Command Syntax

```
show ip rip (database|)
```

Parameters

database	Specify to display information about the IP RIP database.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP
Network Next Hop Metric From If Time
K 0.0.0.0/0 10.0.1.1 16 eth1 01:58
C 10.0.1.0/24 1 eth1
S 10.10.10.0/24 1 eth0
C 10.10.11.0/24 1 eth0
S 192.168.101.0/24 1 eth0
R 192.192.192.0/24 1 --
```

Table 1-125 shows the status codes displayed at the start of a route entry.

Table 1-125: Status codes

Status Code	Meaning	Description
R	RIP	RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
K	Kernel	Kernel is central component of operating system.
C	Connected	Redistribute from locally connected networks.
S	Static	Connections in a static network are fixed links, while connections in a dynamic network are established on the fly as needed.
O	OSPF	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks.

I	IS-IS	Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a host network.
B	BGP	BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.

show ip rip interface

Use this command to display information about RIP interfaces. You can specify an interface name to display information about a specific interface.

Command Syntax

```
show ip rip interface (IFNAME|)
```

Parameters

IFNAME	Name of the interface for which information is to be displayed.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip interface
lo is up, line protocol is up
RIP is not enabled on this interface
eth0 is up, line protocol is up
RIP is not enabled on this interface
eth1 is down, line protocol is down
RIP is not enabled on this interface
eth2 is up, line protocol is up
Routing Protocol: RIP
Receive RIP packets
Send RIPv1 Compatible
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
10.10.1.1/24
10.10.2.1/24
```

Figure 1-126 Explains the show command output details.

Table 1-126: Show ip rip interface output details

Field	Description
Network	IP address of a network entity.
Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.

Metric	If shown, the value of the inter-autonomous system metric.
Routing Protocol	Specifies the routing protocol used.
Passive Interface	Used in all routing protocols to disable sending updates out from a specific interface.
Split horizon	the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.
IP Interface address	IP address of the RIP peer neighbor.

show ip rip statistics

Use this command to display information about RIP statistics. You can specify an interface name to display information about a specific interface.

Command Syntax

```
show ip rip statistics (IFNAME|)
```

Parameters

IFNAME	Name of the interface for which information is to be displayed.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip statistics eth1
Interface Name : eth1
  Sent Multicast Updates  : 3
  Sent Multicast Requests : 1
  Sent Unicast Updates    : 0
  Sent Unicast Requests   : 0
  Recv Multicast Updates  : 3
  Recv Multicast Requests : 0
  Recv Unicast Updates    : 1
  Recv Unicast Requests   : 0
  Recv Bad Packets        : 0
  Recv Bad Routes         : 0
```

Figure 1-127 Explains the show command output details.

Table 1-127: Show ip rip statistics output details

Field	Description
Network	IP address of a network entity.
Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
Metric	If shown, the value of the inter autonomous system metric.
Sent updates	Number of RIP routing updates that have been sent on Multicast/Unicast interface.

Sent Request	Number of RIP routing request that have been sent on Multicast/Unicast interface.
Recv updates	Number of RIP routing updates that have been received on Multicast/Unicast interface.
Recv Request	Number of RIP routing request that have been received on Multicast/Unicast interface.
Recv Bad Packets	Number of packets that were received on this interface and were not processed for any reason.
Recv Bad Routes	Number of route entries that were received on this interface and were not processed for any reason.

snmp restart rip

Use this command to restart SNMP in Routing Information Protocol (RIP)

Command Syntax

```
snmp restart rip
```

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 rip
```

timers basic

Use this command to adjust routing network timers.

This command adjusts the RIP timing parameters. Every 30 seconds, an update is sent out containing the complete routing table to every neighboring router. When the time specified by the timeout parameter expires, the route is no longer valid. However, it is retained in the routing table for a short time so that neighbors are notified that the route has been dropped. When the time specified by the garbage parameter expires, the route is finally removed from the routing table. Until the garbage time expires, the route is included in all updates sent by the router.

All routers in the network must have the same timers to allow RIP to execute a distributed and asynchronous routing algorithms. The timers should not be synchronized as it might lead to unnecessary collisions on the network.

Use the `no` parameter with this command to restore the default routing network timers.

Command Syntax

```
timers basic <5-2147483647> <5-2147483647> <5-2147483647>
no timers basic
```

Parameters

`<5-2147483647>`	Specify the routing table update timer in seconds. The default is 30 seconds.
`<5-2147483647>`	Specify the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
`<5-2147483647>`	Specify the routing garbage collection timer in seconds. The default is 120 seconds.

Default

The default routing table update time is 30 seconds.

The default routing information timeout time is 180 seconds.

The default routing garbage collection time is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#timers basic 30 180 120

(config)#router rip
(config-router)#no timers basic
```

version

Use this command to specify a RIP version used globally by the router. RIP can be run in version 1 as well as version 2 mode. Version 2 has more features than version 1 including authentication. Once the rip version is set, rip packets of that version will be received and sent on all the rip-enabled interfaces.

Use the `no` parameter with this command to restore the default version.

Note: The `ip rip receive version` command and the `ip rip send version` command override the value set by the `version` command.

Command Syntax

```
version <1-2>
no version
```

Parameters

`<1-2>`	Specify the version of RIP processing.

Default

Version 2

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)# network 10.10.11.0/24

#configure terminal
(config)#router rip
(config-router)#address-family ipv4 vrf myVRF
(config-router-af)#version 2
```

CHAPTER 2 RIPng Commands

This chapter provides an alphabetized reference for each of the Routing Information Protocol next generation (RIPng) commands, which support IPv6. It includes the following commands:

aggregate-address

Use this command to set an aggregate RIPng route announcement.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
aggregate-address X:X::X:X/M
no aggregate-address X:X::X:X/M
```

Parameter

`X:X::X:X/M`	Specify an aggregate network (IPv6 address prefix and length).

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#aggregate-address 3ffe:8088::/32

(config)#router ipv6 rip
(config-router)#no aggregate-address 3ffe:8088::/32
```

cisco-metric-behavior

Use this command to enable or disable the metric update as Cisco.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
cisco-metric-behavior (enable|disable)
no cisco-metric-behavior
```

Parameters

`enable`	Enable updating the metric consistent with Cisco.
`disable`	Disable updating the metric consistent with Cisco.

Default

By default, the Cisco metric-behavior is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable the metric update behavior to be consistent with Cisco in the Router mode.

```
#configure terminal
(config)#router ipv6 rip
(config-router)#cisco-metric-behavior enable
```

clear ipv6 rip route

Use this command to clear specific data from the RIPng routing table.

Command Syntax

```
clear ipv6 rip route (X:X::X:X/M|rip|kernel|connected|static|ospf6|isis|bgp|all)
```

Parameters

`X:X::X:X/M`	Removes entries which exactly match this destination address from the RIPng routing table.
`bgp`	Removes only BGP routes from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`isis`	Removes only IS-IS routes from the RIP routing table
`kernel`	Removes kernel entries from the RIP routing table.
`ospf`	Removes only OSPF routes from the RIP routing table.
`static`	Removes static entries from the RIP routing table.
`all`	Removes the entire RIP routing table.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 rip route isis
#clear ipv6 rip route 3ffe:ffff::/16
```

debug ipv6 rip

Use this command to specify the options for the displayed debugging information for RIPng events, RIPng packets and RIPng NSM communications.

Use the `no` option with this command to turn off debugging options for RIPng. The `undebug` alias command can also be used.

Command Syntax

```
debug ipv6 rip (all|)
debug ipv6 rip events
debug ipv6 rip nsm
debug ipv6 rip packet (recv|send|) (detail|)
debug ipv6 rip rib
no debug ipv6 rip (all|)
no debug ipv6 rip events
no debug ipv6 rip nsm
no debug ipv6 rip packet (recv|send|) (detail|)
no debug ipv6 rip rib
undebug ipv6 rip (all|)
undebug ipv6 rip events
undebug ipv6 rip nsm
undebug ipv6 rip packet (recv|send|) (detail|)
undebug ipv6 rip rib
```

Parameters

`all`	Debug all RIP information.
`events`	Debug RIP events.
`nsm`	Debug RIP and NSM communications.
`packet`	Debug RIP packets, only Routing Information Protocol
`recv`	Debug received packets.
`rib`	Debug RIP and RIB communications.
`send`	Debug sent packets.
`detail`	Display detailed information for the sent or received packet.

Default

Disabled

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example specifies the options for the displayed debugging information in `Configure` mode prompt.

```
#configure terminal
(config)#debug ipv6 rip events
(config)#debug ipv6 rip packet send detail
(config)#debug ipv6 rip nsm
```

The following example shows to disable all debugging in `Privileged Exec` mode prompt.

```
#undebug ipv6 rip events
#undebug ipv6 rip packet send detail
#undebug ipv6 rip nsm
```

default-information originate

Use this command to generate a default route into the RIPng.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
default-information originate
no default-information originate
```

Parameters

None

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#default-information originate
```

default-metric

Use this command to specify the metrics to be assigned to redistributed routes.

Use the `no` parameter with this command to disable this feature.

For more details about this command, see the IPv4 version of this command (default-metric).

Command Syntax

```
default-metric <1-15>
no default-metric
```

Parameter

`<1-15>`	Specify the default metric.

Default

By default, the metric value is set to 1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#default-metric 8
```

distance

Use this command to set the administrative distance for RIP.

Use the no option with this command to disable this function.

For more details about this command, see the IPv4 version of this command (distance).

Command Syntax

```
distance <1-255>
no distance (<1-255>|)
```

Parameter

<1-255>	Specify the administrative distance value.

Default

By default, the administrative distance is 120.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 rip
(config-router)#distance 100
```

distribute-list

Use this command to filter incoming or outgoing route updates using the access-list or the prefix-list. You can filter out incoming or outgoing route updates using access-list or prefix-list. If you do not specify the name of the interface, the filter will be applied to all the interfaces.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
distribute-list WORD (in|out) (IFNAME|)
distribute-list prefix WORD (in|out) (IFNAME|)
no distribute-list WORD (in|out) (IFNAME|)
no distribute-list prefix WORD (in|out) (IFNAME|)
```

Parameters

`WORD`	Specify the IPv6 access-list number or name to use.
`prefix`	Filter prefixes in routing updates.
`WORD`	Specify the name of the IPv6 prefix-list to use.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`IFNAME`	Specify the name of the interface on which distribute-list applies.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 rip
(config-router)#distribute-list prefix myfilter in eth0
```

ipv6 rip metric-offset

Use this command to set RIP metric offset.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
ipv6 rip metric-offset <1-16>
no ipv6 rip metric-offset <1-16>
```

Parameter

`<1-16>`	Set a metric value

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 rip metric-offset 1

(config)#interface eth0
(config-if)#no ipv6 rip metric-offset 1
```

ipv6 rip split-horizon

Use this command to perform the split-horizon action on the interface.

Use the `no` parameter with this command to disable this function.

For more details about this command, see the IPv4 version of this command (ip rip split-horizon).

Command Syntax

```
ipv6 rip split-horizon
ipv6 rip split-horizon poisoned
no ipv6 rip split-horizon
```

Parameter

`poisoned`	Performs split-horizon with poisoned reverse.

Default

By default, Split horizon poisoned is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 rip split-horizon

(config)#interface eth1
(config-if)#no ipv6 rip split-horizon
```

ipv6 router rip

Use this command to enable RIPng routing on the interface.

Use the `no` parameter with this command to disable RIPng routing.

Command Syntax

```
ipv6 router rip
no ipv6 router rip
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router rip
```

neighbor

Use this command to specify a neighbor router.

Use the `no` parameter with this command to disable the specific router.

For more details about this command, see the IPv4 version of this command (neighbor).

Command Syntax

```
neighbor X:X::X:X IFNAME
no neighbor X:X::X:X IFNAME
```

Parameters

`X:X::X:X`	Specify a link-local IP address of a neighboring router with which the routing information is exchanged.
`IFNAME`	Specify the name of the interface.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 rip
(config-router)#neighbor 80::1 eth0
```

offset-list

Use this command to add an offset to in and out metrics to routes learned through RIPng.

Use the `no` parameter with this command to remove this function.

For more details about this command, see the IPv4 version of this command (offset-list).

Command Syntax

```
offset-list WORD (in|out) <0-16> (IFNAME|)
no offset-list (WORD) in|out <0-16> (IFNAME|)
```

Parameters

`WORD`	Specify the access-list number or names to apply.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
`<0-16>`	Specify that the offset is used for metrics of networks matching the access list.
`IFNAME`	An alphanumeric string that specifies the interface to match.

Default

The default offset value is the metric value of the interface which is defined by the operating system.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In this example the router examines the RIP updates being sent out from interface eth0 and adds 16 hops to the routes matching the ip addresses specified in the access list `accesslist1`.

```
#configure terminal
(config)#router ipv6 rip
(config-router)#offset-list accesslist1 in 16 eth0
```

passive-interface

Use this command to suppress routing updates on an interface.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

Parameters

`IFNAME`	Specify the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#passive-interface eth0
```

recv-buffer-size

Use this command to run-time configure the RIPng UDP receive-buffer size.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
recv-buffer-size <8192-2147483647>
no recv-buffer-size
```

Parameters

`<8192-2147483647>`

Specify the RIP UDP receive buffer size value.

Default

The default value of the RIP UDP receive-buffer size is 8192.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#recv-buffer-size 150000
```

redistribute

Use this command to redistribute information from other routing protocols.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|ospf|isis|bgp)
redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>
redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD
redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD
no redistribute (kernel|connected|static|ospf|isis|bgp)
no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>
no redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD
no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map
  WORD
```

Parameters

`bgp`	Redistribute from BGP routes
`connected`	Redistribute from connected routes
`isis`	Redistribute from ISO IS-IS routes
`kernel`	Redistribute from kernel routes
`ospf`	Redistribute from OSPF routes (version 3)
`static`	Redistribute from static routes
`metric`	Metric value
`<0-16>`	Specify a metric value
`route-map`	Route map reference
`WORD`	Specify name of the route-map

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#redistribute kernel route-map mymap
(config-router)#redistribute kernel metric 8
```

route

Use this command to debug the specified route advertisement. Use this command to configure static RIPng routes.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
route X:X::X:X/M
no route X:X::X:X/M
```

Parameter

`X:X::X:X/M`	Specify the IPv6 address prefix and length.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#route 3ffe:1234:5678::1/64
```

route-map

Use this command to set a route map for input or output filtering on a specified interface.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
route-map WORD (in|out) IFNAME
no route-map WORD (in|out) IFNAME
```

Parameters

`WORD`	Specify a route map name
`in`	Specify to set the route map for input filtering
`out`	Specify to set the route map for output filtering
`IFNAME`	Specify an interface name to which to associate the route map

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#route-map myRM in eth1
```

router ipv6 rip

Use this global command to enable a RIPng routing process.

Use the `no` parameter with this command to disable the RIPng routing process.

Command Syntax

```
router ipv6 rip
no router ipv6 rip
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#
```

show debugging ipv6 rip

Use this command to display the RIPng debugging status for RIPng NSM, RIPng events, and RIPng packets.

Command Syntax

```
show debugging ipv6 rip
```

Parameters

None

Command Mode

Exec Mode and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ipv6 rip
 RIPng packet debugging is on
```

show ipv6 protocols rip

Use this command to display RIPng process parameters and statistics.

Command Syntax

```
show ipv6 protocols rip
```

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 the `show ipv6 protocols rip` command.

```
#show ipv6 protocols rip
Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-50%, next due in 10 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 redistribute metric is 1
  Redistributing: connected
  Routing for Networks:
    3ffe:1::/64
#
```

show ipv6 rip

Use this command to show RIP routes.

Command Syntax

```
show ipv6 rip (database|)
```

Parameters

`database`	Specify to display information about the IPv6 RIP database.

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 ipv6 rip database command.

```
#show ipv6 rip database
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP, a - aggregate, s - suppressed
Network Next Hop If Met Tag Time
R 3ffe:1234:5678::/64 fe80::3 eth1 3 0 02:28
C 3ffe:ffff:1::/64 :: eth0 1 0
Ra 3ffe:ffff:2::/48 -- 1 0
Rs 3ffe:ffff:2::/48 fe80::3 eth1 3 0 02:32
Cs 3ffe:ffff:2::/64 :: eth1 1 0
R 3ffe:ffff:ffff:ffff::/64 fe80::3 eth1 3 0 02:28
```

show ipv6 rip interface

Use this command to display information about the RIPng interfaces. You can specify an interface name to display information about a specific interface.

Command Syntax

```
show ipv6 rip interface (IFNAME|)
```

Parameters

IFNAME	Name of the interface for which information is 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 from the `show ipv6 rip interface` command.

```
#show ipv6 rip interface
lo is up, line protocol is up
RIPng is not enabled on this interface
eth0 is up, line protocol is up
RIPng is not enabled on this interface
eth1 is down, line protocol is down
RIPng is not enabled on this interface
eth2 is up, line protocol is up
Routing Protocol: RIPng
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
3ffe:ffff::1/64
3ffe:fffe::1/64
```

timers basic

Use this command to adjust routing network timers.

Use the `no` parameter with this command to restore the defaults.

For more details about this command, see the IPv4 version of this command (timers basic).

Command Syntax

```
timers basic <5-2147483647> <5-2147483647> <5-2147483647>
no timers basic
```

Parameters

`<5-2147483647>`	Specify the routing table update timer in seconds. The default is 30 seconds.
`<5-2147483647>`	Specify the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
`<5-2147483647>`	Specify the routing garbage collection timer in seconds. The default is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#timers basic 30 180 120

(config)#router ipv6 rip
(config-router)#no timers basic
```

CHAPTER 3 Routing Information Protocol VPN Commands

This chapter provides information about RIP VPN commands. These commands are available when the RIP Provider Edge (PE) and Customer Edge (CE) feature is supported. Using these commands, VPN you can use RIP to receive information which the CE-router places into the connected Virtual Routing and Forwarding (VRF) from the receiving interface. The information is then advertised across the MPLS/VPN backbone between PE-routers.

To provide a VPN service, the PE-router needs to be configured so that any routing information learned from a VPN customer interface can be associated with a particular VRF. This is achieved using any standard routing protocol process (RIP, OSPF, BGP or static routes etc).

To enable the RIP PE-CE feature, an Address Family sub-mode is used. Most of the RIP commands that are available in Router and Interface mode are also available in Address Family mode. Additionally, all RIP debug commands display additional VRF information when the RIP PE-CE feature is supported.

This chapter contains the following commands:

address-family ipv4 vrf

Use this command to enable the exchanging of VRF routing information and to enter the Address Family mode. This command configures the routing exchange between PE and CE devices. Configure a RIP address family for each VRF configured on the PE router.

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 RIP process using this command.

Use the `no` parameter with this command to disable it.

Command Syntax

```
address-family ipv4 vrf NAME
no address-family ipv4 vrf NAME
```

Parameters

`NAME`	Specify the name for the VRF instance

Default

None

Command Mode

Router mode

OcNOS version 1.3

This command was introduced before OcNOS version 1.3.

Examples

The following example places the router in Address Family mode and specifies VRF1 as the name of the VRF instance to associate with subsequent IP Version 4 Address Family mode commands:

```
#configure terminal
(config)#router rip
(config-router)#address-family ipv4 vrf VRF1
(config-router-af)#
```

exit-address-family

Use this command to exit the Address Family mode. This command is supported in RIP (IPv4).

Command Syntax

```
exit-address-family
```

Parameters

None

Default

None

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show the change in prompt after using the `exit-address-family` command to exit the `Address Family` mode.

```
(config)#router rip
(config-router)#address-family ipv4 vrf myVRF
(config-router-af)#exit-address-family
(config-router)#
```

show ip rip interface vrf

Use this command to display VRF information. This command is supported in RIP (IPv4).

Command Syntax

```
show ip rip interface vrf WORD (IFNAME|)
```

Parameters

WORD	Specify the name for the VRF instance.
IFNAME	Specify name for the interface.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip rip interface vrf myVRF

eth1 is up, line protocol is up
  Routing Protocol: RIP
    VPN Routing/Forwarding: myVRF
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      1.1.1.92/24
eth3 is up, line protocol is up
  RIP is not enabled on this interface
```

Figure 3-128 Explains the show command output details.

Table 3-128: Show ip rip interface vrf output details

Field	Description
Routing Protocol	Specifies the routing protocol used.
VPN Routing/Forwarding	Specifies the name of the virtual routing and forwarding (VRF) instance.
Receive RIP packets	Number of RIP packets that were received on this interface.
Send RIP packets	Number of RIP packets that were send on this interface.
Passive Interface	Used in all routing protocols to disable sending updates out from a specific interface.

Split horizon	the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.
IP Interface address	IP address of the RIP peer neighbor.

show ip rip vrf

Use this command to display VRF information. This command is supported in RIP (IPv4).

Command Syntax

```
show ip rip (database) vrf WORD
```

Parameters

`database`	Specify to display information about the IP RIP database.
`WORD`	Specify the name for the VRF instance.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip rip database vrf myVRF
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If     Time
Rc 1.1.1.0/24                              1                  eth1
S  72.72.75.0/24      98.98.8.2            1                  eth3
```

Table 3-129 shows the status codes displayed at the start of a route entry.

Table 3-129: Status codes

Status Code	Meaning	Description
R	RIP	RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
Rc	RIP Connected	Redistribute from locally RIP connected networks.
Rs	RIP Static	Connections in a RIP static network are fixed links, while connections in a dynamic network are established on the fly as needed.
K	Kernel	Kernel is central component of operating system.
C	Connected	Redistribute from locally connected networks.

Rs	RIP Static	Connections in a RIP static network are fixed links, while connections in a dynamic network are established on the fly as needed.
O	OSPF	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks.
I	IS-IS	Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a host network.
B	BGP	BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.
	Network	IP address of a network entity.
	Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
	Metric	If shown, the value of the inter-autonomous system metric.

Figure 3-130 Explains the show command output details.

Table 3-130: Show ip rip vrf output details

Field	Description
Network	IP address of a network entity.
Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
Metric From	If shown, the value of the inter-autonomous system metric.
If	Ethernet interface.
Time	Specifies the time between forwarding packets.

show ip vrf

Use this command to display VRF information. This command is supported in RIP (IPv4).

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameters

WORD	Specify the name for the VRF instance.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip vrf myVRF

VRF myVRF, FIB ID 1
Router ID: 1.1.1.2 (config)
Interfaces:
  eth1
  eth3
VRF myVRF; (id=1); RIP enabled Interfaces:
  eth1
```

Appendix A Routing Information Protocol Authentication

To support RIPv2 message authentication, you can choose plain text or MD5 authentication, with the option for a single key or multiple keys in different modes and stages.

Single Key Authentication

Use the following steps to configure route to enable RIPv2 authentication using a single key or password:

1. Define the authentication string or password

   In the Interface mode, specify the authentication string or password used by the key using the following command:

   ```
   ip rip authentication string LINE
   ```

   where `LINE` is the authentication string or password

2. Specify mode of authentication for the interface

   In the Interface mode, specify either text or MD5 authentication using the following command:

   ```
   ip rip authentication mode md5|text
   ```

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip authentication string mykey
(config-if)#ip rip authentication mode md5
```

Multiple Keys Authentication

Use the following steps to configure route to enable RIPv2 authentication using multiple keys at different times:

1. Define a key chain

   In the Configure mode, identify a key chain with a key chain name using the following command:

   ```
   key chain KEYNAME
   ```

   where `KEYNAME` is the name of the chain to manage.

2. Define the key(s)

   In the Keychain mode, specify a key on this key chain using the following command:

   ```
   key KEYID
   ```

   where `KEYID` = `<0-2147483647>` Key Identifier number

3. Define the authentication string or password

   In the Keychain-key mode, define the password used by a key, using the following command:

   ```
   key-string LINE
   ```

   where `LINE` is a string of characters to be used as a password by the key.

4. Set key management options

   This step can be performed at this stage or later when multiple keys are used. The options are configured in the `keychain-key` command mode.

- Set the time period during which the authentication key on a key chain is received as valid, using the following command:

  ```
  accept-lifetime START END
  ```

  where `START` and `END` are the beginning and end of the time period.

- Set the time period during which the authentication key on a key chain can be sent using the following command:

  ```
  send-lifetime START END
  ```

  where `START` and `END` are the beginning and end of the time period.

5. Enable authentication on an interface

   In the Interface mode, enable authentication on an interface and specify the key chain to be used, using the following command:

   ```
   ip rip authentication key-chain CHAINNAME
   ```

   where `CHAINNAME` is a set of valid authentication keys

6. Specify mode of authentication for the interface

   In the Interface mode, specify either text or MD5 authentication using the following command:

   ```
   ip rip authentication mode md5|text
   ```

Example

In the following example, a password `toyota` is set for a `key 1` in a key chain `cars`. On Interface `eth0` authentication is enabled and the authentication mode is set as `MD5`.

```
#configure terminal
(config)#key chain cars
(config-keychain)#key 1
(config-keychain-key)#key-string toyota
(config-keychain-key)#accept-lifetime 10:00:00 Oct 08 2002 duration 43200
(config-keychain-key)#send-lifetime 10:00:00 Oct 8 2002 duration 43200
(config-keychain-key)#exit
(config-keychain)#exit
(config)#interface eth0
(config-if)#ip rip authentication key-chain cars
(config-if)#ip rip authentication mode md5
(config-if)#exit
```

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 rfc1771-path-select
- bgp rfc1771-strict
- bgp router-id
- bgp scan-time
- bgp table-map
- bgp update-delay
- 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 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 additional-paths
- neighbor advertise additional-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor allowas-in
- neighbor as-origination-interval

- neighbor attribute-unchanged
- neighbor capability dynamic
- neighbor capability graceful-restart
- 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 filter-list
- neighbor g-shut
- neighbor g-shut-timer
- neighbor limit
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor optional-as
- neighbor override-capability
- neighbor passive
- neighbor password
- neighbor peer-group
- neighbor peer-group range
- neighbor prefix-list
- neighbor remote-as
- neighbor remove-private-AS
- neighbor restart-time
- 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 unsuppress-map
- neighbor update-source
- neighbor version
- neighbor weight
- neighbor WORD peer-group
- network
- network synchronization
- redistribute
- restart bgp gracefull
- router bgp
- snmp restart bgp
- synchronization
- timers bgp
- undebug 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 the address family mode and return to the Configure mode use 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 l2vpn evpn
address-family rtfilter unicast
address-family vpn4
address-family vpn4 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
```

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
`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

Applicability

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

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
```

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

No default value is specified

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

No default value is specified

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 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 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 RIP, 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.

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 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 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 filter for BGP for an 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 filter for BGP for an IPv6 address family.

```
(config)#router bgp 100
(config-router)#address-family ipv6
(config-router-af)# table-map abc filter
```

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
```

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|WORD)
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.
`WORD`	Interface name
`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.

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.

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.

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.

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.

Command Syntax

```
clear ip bgp (A.B.C.D|WORD) in
clear ip bgp A.B.C.D in prefix-filter
clear ip bgp (A.B.C.D|WORD) out
clear ip bgp (A.B.C.D|WORD) soft
clear ip bgp (A.B.C.D|WORD) soft in
clear ip bgp (A.B.C.D|WORD) 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

`A.B.C.D`	IPv4 address
`WORD`	Interface 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.
`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.

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 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 dampening
no debug bgp events
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-vrf, Address-Family-vpnv4 mode.

For information on how to enter the address family mode (IPv4, VPNv4), see address-family.

Command Syntax

```
exit-address-family
```

Parameters

None

Default

No default value is specified

Command Mode

Address Family-vrf and Address Family-vpnv4 mode.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples shows the change in the prompt after using this command.

```
#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

No default value is specified

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 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 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|WORD) activate
no neighbor (A.B.C.D|WORD) activate
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 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

Address Family mode and Router 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 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 peer group.

Note: For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified 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, default number of local AS is 3

Command Mode

Router mode and 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 and 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 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 and 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 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

Use this command to advertise to peer about route refresh capability. If route refresh capability is supported, then router can dynamically request that the peer re-advertises its Adj-RIB-Out.

Use the `no` parameter with this command to disable this function

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh
no neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh
```

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 route refresh 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 route-refresh
```

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 and Address Family

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 and 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 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 and 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 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 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> <1-100>
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100> warning-only
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> 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> 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
`<1-100>`	Threshold value percent <1-100>
`warning-only`	Only give a warning message when the limit 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.

Default

By default, neighbor maximum prefix is disabled

Command Mode

Router mode and 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. The 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 and 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 password

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) password <WORD>
no neighbor (A.B.C.D|X:X::X:X|WORD) password <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 the BGP peer group
`WORD`	Password (Maximum length is 80 characters)

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 bgp 11
(config-router)#neighbor 10.10.0.73 password myPass

(config-router)#no neighbor 10.10.0.73 password 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.

See Usage below for when a peer group and a neighbor have conflicting attribute configurations.

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 IPv4 format
X:X::X:X	Address of the BGP neighbor in IPv6 format
WORD	Peer group name

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 bgp 10
(config-router)#neighbor group1 peer-group
```

Usage

When a *peer group* and a *peer* (neighbor) have conflicting attribute configurations the following rules apply:

- Outbound attribute configurations of a peer group *replace* peer member configurations of the same attributes when a peer becomes member of that peer group. Outbound attribute modifications to group members are not allowed.
- A peer group member's inbound attribute configurations take precedence over the peer group configuration.

These commands control outbound attribute updates:

- neighbor activate
- neighbor additional-paths
- neighbor advertisement-interval
- neighbor as-origination-interval

- neighbor attribute-unchanged
- neighbor capability orf prefix-list
- neighbor distribute-list with an access-list number and the `out` parameter
- neighbor dont-capability-negotiate
- neighbor fall-over bfd (BGP)
- neighbor filter-list with the `out` parameter
- neighbor next-hop-self
- neighbor prefix-list with an access-list name and the `out` parameter
- neighbor remove-private-AS
- neighbor route-map with the `out` parameter
- neighbor route-reflector-client
- neighbor route-server-client
- neighbor send-community
- neighbor send-label explicit-null
- neighbor unsuppress-map

These commands control inbound attribute updates:

- neighbor allowas-in
- neighbor collide-established
- neighbor description
- neighbor distribute-list with an access-list number and the `in` parameter
- neighbor ebgp-multihop
- neighbor enforce-multihop
- neighbor filter-list with the `in` parameter
- neighbor g-shut
- neighbor g-shut-timer
- neighbor local-as
- neighbor maximum-prefix
- neighbor override-capability
- neighbor passive
- neighbor password
- neighbor port
- neighbor prefix-list with an access-list name and the `in` parameter
- neighbor remote-as
- neighbor restart-time
- neighbor route-map with the `in` parameter
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor strict-capability-match

- neighbor update-source
- neighbor weight

neighbor peer-group range

Use this command to create a dynamic peer group.

Use the no parameter with this command to remove a peer group.

Command Syntax

```
neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M)
no neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M)
```

Parameters

`A.B.C.D/M`	IP Prefix
`X:X::X:X/M`	IPv6 Prefix
`WORD`	Peer group name

Default

No default value is specified

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 10
(config-router)#neighbor group1 peer-group range 10.10.10.0/24
```

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

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 and 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.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) remote-as (<1-4294967295>|internal|external)
no neighbor (A.B.C.D|X:X::X:X|WORD) remote-as (<1-4294967295>|internal|external)
```

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. For an unnumbered interface (RFC 5549), specify an interface name configured with neighbor discovery or an IPv4 address with /31 or /30.
`<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.
`internal`	iBGP peer.
`external`	eBGP peer.

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 and updated in OcNOS version 1.3.6.

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 and 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 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
```

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

No default value is specified

Command Mode

Router mode and 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

No default value is specified

Command Mode

Router mode and 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

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 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 2, *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 and 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 and 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 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 and 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

No default value is specified

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

No default value is specified

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
```

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
```

router bgp

Use this command to start a BGP process.

Use the `no` parameter with 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

No default value is specified

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

No default value is specified

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

No default value is specified

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
```

undebug bgp

Use this command to disable BGP debugging options.

Command Syntax

```
undebug bgp (all|bfd|dampening|events|filters|fsm|keepalives|mpls|nht|nsm|updates)
```

Parameters

`all`	Disable all debugging for BGP
`bfd`	Disable debugging for BGP Bidirectional Forwarding Detection (BFD)
`dampening`	Disable debugging for BGP dampening
`events`	Disable debugging for BGP events
`filters`	Disable debugging for BGP filters
`fsm`	Disable debugging for BGP Finite State Machine (FSM)
`keepalives`	Disable debugging for BGP keepalives
`mpls`	Disable debugging for BGP MPLS
`nht`	Disable debugging for BGP NHT messages
`nsm`	Disable debugging for NSM messages
`updates`	Disable debugging for BGP updates

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#undebug bgp events
```

CHAPTER 2 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*)
- import map
- 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.

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.

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.

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
```

import map

This command assigns a route map to the VRF. This map is applied for routing information imported from another PE or VRF.

Use this command when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities. You can filter routes that are eligible for import into a VRF through the use of a route map.The route map can deny access to selected routes from a community that is on the import list.

Use the `no` option with this command to remove the map.

Command Syntax

```
import map WORD
no import map
```

Parameter

`WORD`	Route map

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf myVRF
(config-vrf)#import map set-pref
(config-vrf)#
```

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 3 BGP Show Commands

This chapter describes the BGP show commands.

- show ip bgp peer-group
- show ip bgp peer-group vrf all
- show ip bgp rtfilter all
- show ip bgp scan
- show ip bgp vpnv4
- show ip extcommunity-list
- show ip extcommunity-list
- show ip protocols
- show ip vrf
- show running-config as-path access-list
- show running-config community-list

show bgp

Use this command to display the status of BGP routes.

Command Syntax

```
show bgp
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
```

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 3-131 explains the output fields.

Table 3-131: 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 3-131: 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

```
#show bgp client
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 bgp dampening dampened-paths
```

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
```

Header

```
BGP table version is 1, local router ID is 30.30.30.77
```

- BGP table version
- BGP router ID is `30.30.30.77`

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale
```

Table 3-131 shows the status codes displayed at the start of a route entry.

Table 3-132: 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 3-133 shows the codes at the end of each route entry that indicate where the route originated.

Table 3-133: 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 3-134 explains the output fields.

Table 3-134: 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).

Table 3-134: show bgp dampening flap-statistics output details

Field	Description
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.

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 3-135 explains the output fields.

Table 3-135: 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 3-136 shows the status codes displayed at the start of a route entry.

Table 3-136: 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 3-137 shows the codes at the end of each route entry that indicate where the route originated.

Table 3-137: 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 3-138 explains the output fields.

Table 3-138: 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.
Local Pref	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 before 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 3-139 explains the output fields.

Table 3-139: 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 3-139: 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 3-140 explains the output fields.

Table 3-140: 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 neighbors (A.B.C.D|X:X::X:X|WORD)
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)(advertised-routes|)
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD)
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) (hold-time|keepalive-
  interval|connection-retrytime)
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) (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
`WORD`	Interface name
`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 3-141 explains the output fields.

Table 3-141: 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.

Table 3-141: show bgp neighbor output details

Field	Description
local AS	Local Autonomous system used to exchange internal routing information within AS.
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 3-146. 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.

Table 3-141: show bgp neighbor output details

Field	Description
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.
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|WORD) 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|WORD) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes advertised
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD) advertised-
  routes
```

Parameters

`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`WORD`	Interface name
`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|WORD) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) 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
`WORD`	Interface name
`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|WORD) 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|WORD) received-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes received
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`WORD`	Interface name
`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|WORD) routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD) routes
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`WORD`	Interface name
`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 3-142 explains the output fields.

Table 3-142: 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: • Route refresh • Address family IPv4 Unicast • 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 3-143 explains the output fields.

Table 3-143: 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 3-143: 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 3-144 explains the output fields.

Table 3-144: 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 3-145 explains the output fields.

Table 3-145: 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 3-146 explains the fields for each neighbor entry.

Table 3-146: 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 3-146: 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
```

Table 3-147 explains the status codes in the header.

Table 3-147: 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 3-148 explains the codes are at the end of each routing entry that show where the route originated.

Table 3-148: 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 3-149 explains the fields shows for each route.

Table 3-149: 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 3-147.
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	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 3-149

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 3-150 explains the status codes in the header.

Table 3-150: 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 3-151 explains the codes are at the end of each routing entry that show where the route originated.

Table 3-151: 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 3-152 explains the fields shows for each route.

Table 3-152: 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 3-150.
Next Hop	IP address of the nexthop for this route.

Table 3-152: route entry fields (Continued)

Field	Description
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	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 3-151

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 attribute-info

Use this command to show internal attribute hash information.

Command Syntax

```
show ip bgp attribute-info
```

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 ip bgp attribute-info` command displaying internal attribute information.

```
#show ip bgp attribute-info
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.10.10.10
```

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
```

Table 3-153 explains the status codes in the header.

Table 3-153: 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.

Table 3-153: status codes (Continued)

*	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 3-154 explains the codes are at the end of each routing entry that show where the route originated.

Table 3-154: 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 3-155 explains the fields shows for each route.

Table 3-155: 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 3-153.
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	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 3-154

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 3-156 explains the fields shows for each route.

Table 3-156: 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: • Route refresh • Address family IPv4 Unicast • 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 3-156: 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 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 3-157 explains the fields shows for each route.

Table 3-157: 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 3-157: 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)
```

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)#
```

Appendix A Regular Expressions

Table A-158 shows the regular expression special characters used in BGP commands. You can use these characters in combination to build complex regular expressions.

Table A-158: 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.

SECTION 6 # 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 1-19.

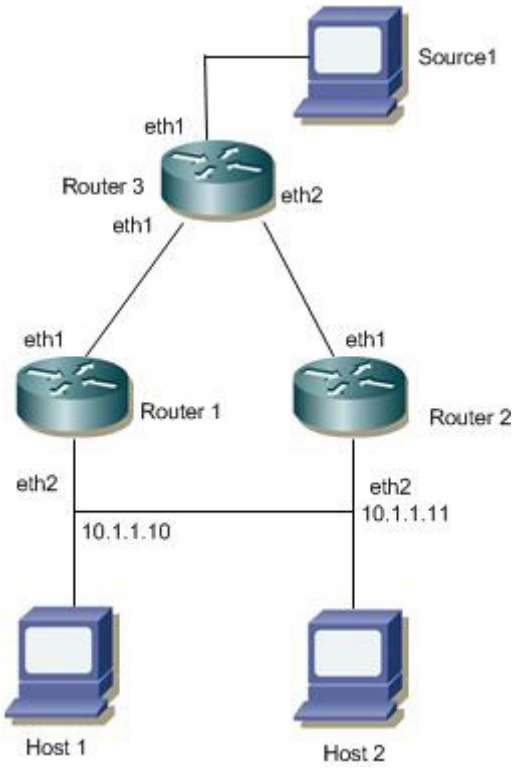


Figure 1-19: IGMP Topology

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 1-159: 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      Last Reporter
  224.0.1.3            eth2       00:10:06   00:03:43     10.1.1.52
  224.1.1.1            eth2       01:54:53   static         0.0.0.0
  225.1.1.1            eth2       00:17:22   static         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 1-160: 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 mrouter 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.

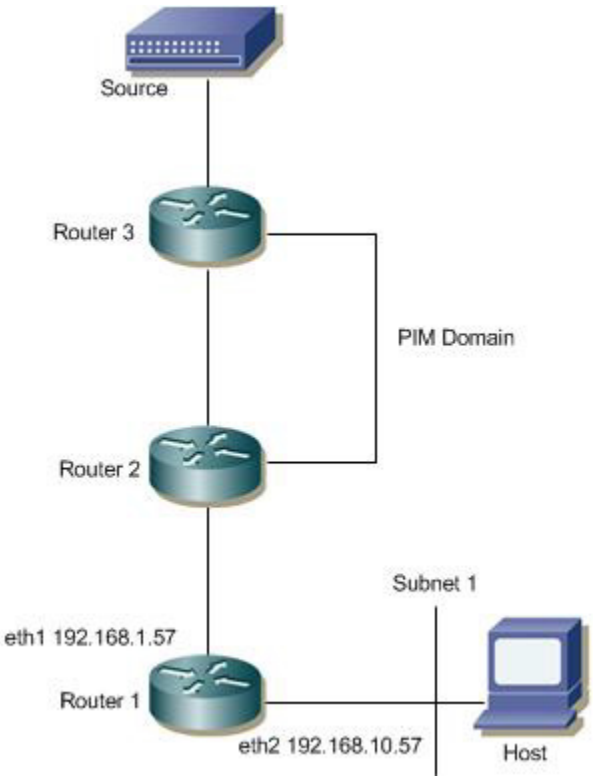


Figure 2-20: IGMP Proxy Topology

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 mrouter 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 mrouter-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.

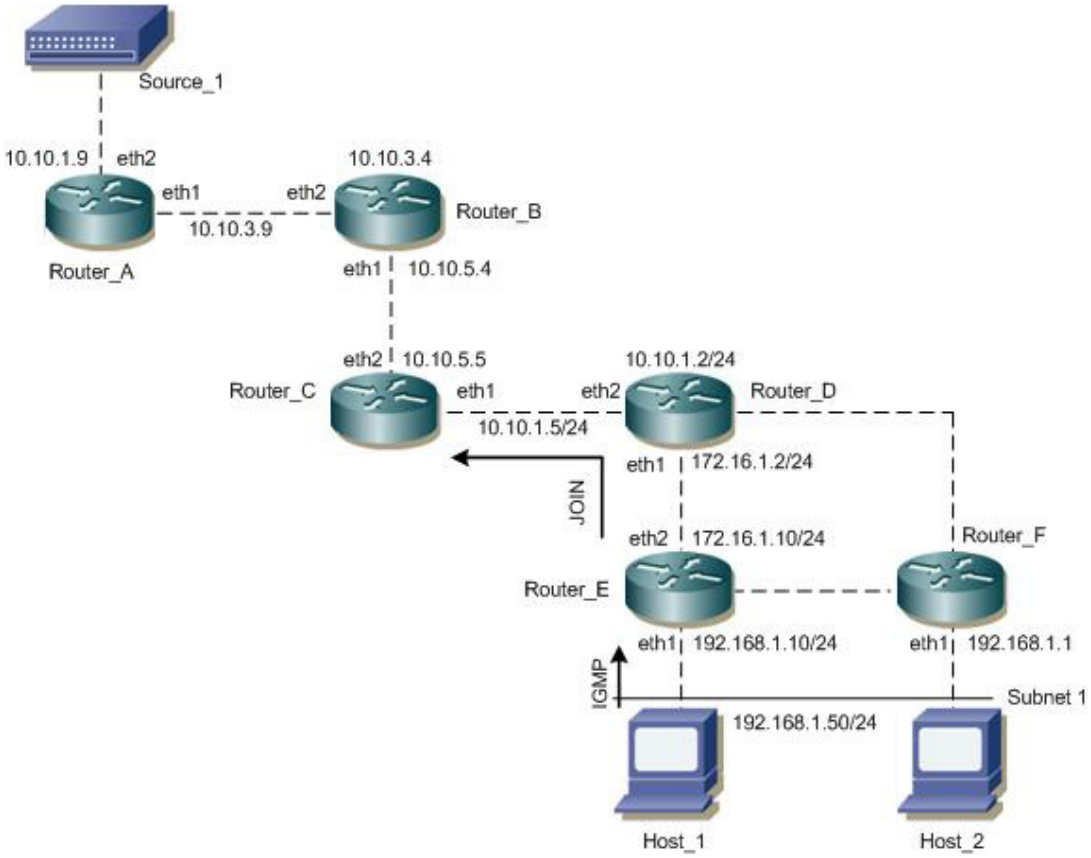


Figure 3-21: PIM-SM Topology

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 3-21, `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 3-22 for the topology.

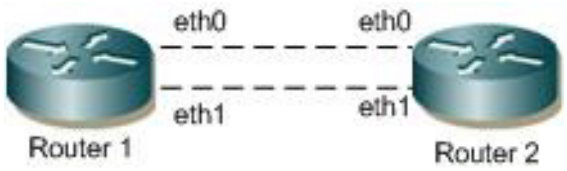


Figure 3-22: Boostrap Router Topology

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

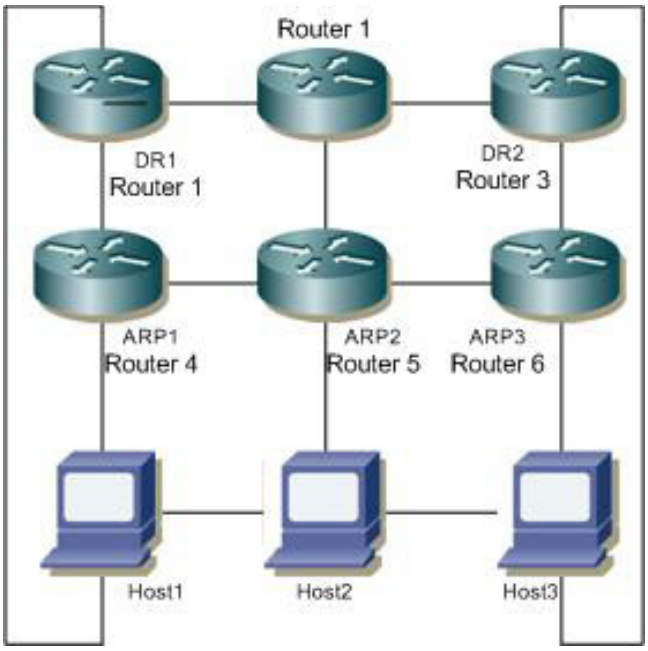


Figure 3-23: Anycast RP Topology

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.

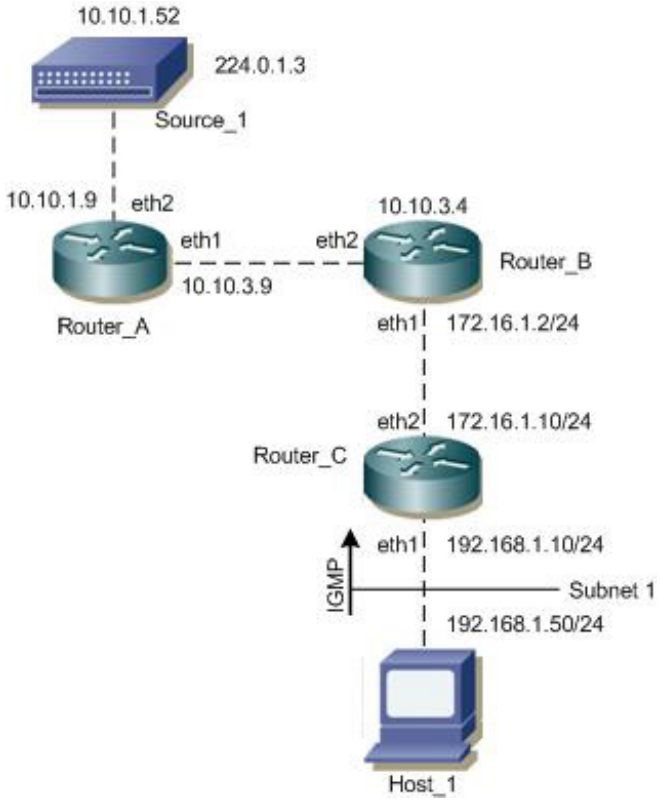


Figure 4-24: PIM-DM Configuration Topology

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.

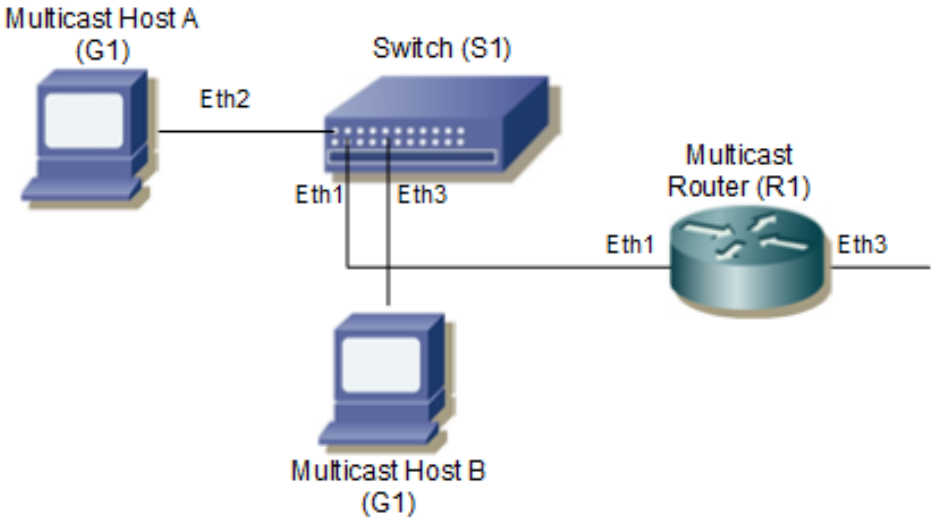


Figure 5-25: IGMP Snooping Topology

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)#vlan database`	enter VLAN mode
`(config-vlan)# vlan 2 bridge 1`	Create VLAN and add it to bridge 1
`(config)#exit`	Exit VLAN mode
`(config)#interface eth3`	Specify the interface `eth3` to be configured, and Enter 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 trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit 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 trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit 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 trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface vlan1.2`	Specify interface `vlan1.1` to be configured.
`(config)#ip address 1.2.3.4/24`	Specify IP address

(config-if)# igmp snooping mrouter interface eth1	Configure this port as a multicast router port
(config-if)#exit	Exit interface mode

Validation

```
#show running-config interface eth3
!
interface eth3
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#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
2 224.1.1.1 eth3 R 00:00:03 00:04:17 0.0.0.0 V3
2 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0 V3

#show igmp snooping interface vlan1.2
IGMP Snooping information for vlan1.2
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 enabled
IGMPv3 Report suppression enabled
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:
Eth3
Eth1
```

```
    Eth2
```

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 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 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
```

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
```

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
```

Table 1-161: 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 1-162: 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.

Table 1-162: Show ip mroute output

Entry	Description
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 1-163: 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 1-164: 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 1-164: 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 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
!
```

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 L3 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 4, *L2 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 2-165 shows the flags codes displayed at the start of a group entry.

Table 2-165: Flags

Flag	Meaning
M	Source Specific Multicast
R	Remote multicast
L	Local multicast
SG	Static Group
SS	Static Source

Table 2-166 explains the output fields.

Table 2-166: 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 2-165.
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 2-165.
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 2-165.

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 2-167 explains the output fields.

Table 2-167: 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 2-167: 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 2-168 explains the output fields.

Table 2-168: 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 2-169 explains the output fields.

Table 2-169: 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
```

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
!
```

CHAPTER 3 MLD Multicast Commands

This chapter describes the commands for Multicast Listener Discovery (MLD) which includes the MLD proxy service.

clear ipv6 mld

Use this command to clear MLD local memberships in an interface or group. This command applies to entities configured for MLD layer-3 multicast protocols, or MLD proxy.

Command Syntax

```
clear ipv6 mld
clear ipv6 mld group *
clear ipv6 mld group X:X::X:X
clear ipv6 mld group X:X::X:X IFNAME
clear ipv6 mld group [*|X:X::X:X (IFNAME)]
clear ipv6 mld interface IFNAME
clear ipv6 mld (vrf NAME|)
clear ipv6 mld (vrf NAME|) group *
clear ipv6 mld (vrf NAME|) group X:X::X:X
clear ipv6 mld (vrf NAME|) group X:X::X:X IFNAME
clear ipv6 mld (vrf NAME|) interface IFNAME
```

Parameter

`vrf`	Specify the VRF name.
`groups`	Clears groups from an interface.
`*`	Clears all groups from an interface.
`X:X::X:X`	Specify an IPv6 interface.
`interface`	Specify the interface parameter.
`IFNAME`	Specify the interface name.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 mld group *
#clear ipv6 mld group 224.1.1.1
#clear ipv6 mld vrf VRF_A
```

debug ipv6 mld

Use this command to enable debugging of all MLD, or a specific component of MLD. This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Use the `no` parameter with this command to disable all MLD debugging or debugging of a specific component of MLD.

Command Syntax

```
debug ipv6 mld all
debug ipv6 mld decode
debug ipv6 mld encode
debug ipv6 mld events
debug ipv6 mld fsm
debug ipv6 mld tib
debug ipv6 mld (vrf NAME|) all
debug ipv6 mld (vrf NAME|) decode
debug ipv6 mld (vrf NAME|) encode
debug ipv6 mld (vrf NAME|) events
debug ipv6 mld (vrf NAME|) fsm
debug ipv6 mld (vrf NAME|) tib
no debug ipv6 mld all
no debug ipv6 mld decode
no debug ipv6 mld encode
no debug ipv6 mld events
no debug ipv6 mld fsm
no debug ipv6 mld tib
no debug ipv6 mld (vrf NAME|) all
no debug ipv6 mld (vrf NAME|) decode
no debug ipv6 mld (vrf NAME|) encode
no debug ipv6 mld (vrf NAME|) events
no debug ipv6 mld (vrf NAME|) fsm
no debug ipv6 mld (vrf NAME|) tib
```

Parameters

`all`	Debug all MLD.
`decode`	Debug MLD decoding.
`encode`	Debug MLD encoding.
`events`	Debug MLD events.
`fsm`	Debug MLD finite state machine (FSM).
`tib`	Debug MLD 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 mld all
```

ipv6 mld

Use this command to enable the MLD protocol operation on an interface. This command enables MLD protocol 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 MLD Proxy.

Note: This command can only be issued on VLAN interfaces.

Use the `no` parameter with this command to return all MLD related configuration to the default or MLD Proxy service.

Command Syntax

```
ipv6 mld
no ipv6 mld
```

Parameters

None

Default

Disabled

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 mld
```

ipv6 mld access-group

Use this command to control the multicast local-membership groups learnt on an interface. This command applies to interfaces configured for MLD layer-3 multicast protocols, or MLD proxy.

Note: This command can only be issued on VLAN interfaces.

Use the `no` parameter with this command to disable this access control.

Command Syntax

```
ipv6 mld access-group WORD
no ipv6 mld access-group
```

Parameter

`WORD`	Standard IPv6 access-list name.

Default

No access list configured.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can join the group `ff0e::1/128` only:

```
#configure terminal
(config)#ipv6 access-list Group1 permit ff0e::1/128
(config)#interface fxp0
(config-if)#ipv6 mld access-group Group1
```

ipv6 mld immediate-leave

Use this command to minimize the leave latency of MLD memberships. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy. Use this command when only one receiver host is connected to each interface.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
ipv6 mld immediate-leave group-list WORD
no ipv6 mld immediate-leave
```

Parameter

`group-list`	Standard IPv6 access-list name that defines multicast groups in which the immediate leave feature is enabled.

Default

Disabled

Command Mode

Interface mode for VLAN interface

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 node membership at a time per interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld immediate-leave v6grp
(config-if)#exit
```

ipv6 mld last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax

```
ipv6 mld last-member-query-count <2-7>
no ipv6 mld last-member-query-count
```

Parameters

`<2-7>`	Specify a last-member query-count value.

Default

The default last-member query-count value is 2.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld last-member-query-count 3
```

ipv6 mld last-member-query-interval

Use this command to set the frequency at which the router sends MLD group-specific host query messages. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to set this frequency to the default value.

Command Syntax

```
ipv6 mld last-member-query-interval <1000-25500>
no ipv6 mld last-member-query-interval
```

Parameter

`<1000-25500>`	Specify a last member query interval value in milliseconds.

Default

The default last-member query-count value is 1000 milliseconds.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the MLD group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld last-member-query-interval 2000
```

ipv6 mld limit

Use this command to set the limit on the maximum number of group membership states at either the router level, or for the specified interface. Once the specified number of group memberships is reached, all further local-memberships will be 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 MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax

```
ipv6 mld limit <1-2097152> (except WORD |)
ipv6 mld (vrf NAME|) limit <1-2097152> (except WORD |)
no ipv6 mld limit
```

Parameters

`vrf`	Specify the VRF name.
`<1-2097152>`	Maximum number of group membership states.
`except`	Standard IPv6 access-list name that defines multicast groups which are exempted from being subject to the configured limit.
`WORD`	Specify the standard IPv6 access-list name.

Default

The default value is 0 (zero).

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures an MLD limit of 100 group-membership states across all interfaces on which MLD is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
(config)#ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on eth0:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld limit 100
```

ipv6 mld mroute-proxy

Use this command to specify the MLD Proxy service (upstream host-side) interface with which to be associated. MLD router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional. This command should not be configured on interfaces enabled for MLD 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

```
ipv6 mld mroute-proxy IFNAME
no ipv6 mld mroute-proxy
```

Parameters

`IFNAME`	Specify the interface name.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the eth0 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 mld mroute-proxy eth0
```

ipv6 mld proxy-service

Use this command to designate an interface to be the MLD proxy-service (upstream host-side) interface, thus enabling MLD host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to MLD host-side functionality.

This command should not be used when configuring interfaces enabled for MLD 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

```
ipv6 mld proxy-service
no ipv6 mld proxy-service
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example designates the eth0 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld proxy-service
```

ipv6 mld querier-timeout

Use this command to configure 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 MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ipv6 mld querier-timeout <60-300>
no ipv6 mld 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.

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 eth0
(config-if)#ipv6 mld querier-timeout 120
```

ipv6 mld query-interval

Use this command to set the frequency of sending MLD host query messages. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default frequency.

Command Syntax

```
ipv6 mld query-interval <1-18000>
no ipv6 mld query-interval
```

Parameter

`<1-18000>`	Frequency (in seconds) at which MLD host query messages are sent.

Default

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 MLD host-query messages to 2 minutes:

```
#configure terminal
(config)#interface fxp0
(config-if)#ipv6 mld query-interval 120
```

ipv6 mld query-max-response-time

Use this command to set the maximum response time advertised in MLD queries. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ipv6 mld query-max-response-time <1-240>
no ipv6 mld query-max-response-time
```

Parameter

`<1-240>`	Maximum response time (in seconds) advertised in MLD 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 eth0
(config-if)#ipv6 mld query-max-response-time 8
```

ipv6 mld robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax

```
ipv6 mld robustness-variable <2-7>
no ipv6 mld robustness-variable
```

Parameter

`<2-7>`	Specify a robustness variable value in seconds.

Default

Default robustness value is 2 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld robustness-variable 3
```

ipv6 mld ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax

```
ipv6 mld ssm-map enable
ipv6 mld (vrf NAME|) ssm-map enable
no ipv6 mld ssm-map enable
no ipv6 mld (vrf NAME|) ssm-map enable
```

Parameter

`vrf`	Specify the VRF name.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable MLD SSM mapping on the router.

```
#configure terminal
(config)#ipv6 mld ssm-map enable
```

ipv6 mld ssm-map static

Use this command to specify the static mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to remove the SSM map association.

Command Syntax

```
ipv6 mld ssm-map static WORD X:X::X:X
ipv6 mld (vrf NAME|) ssm-map static WORD X:X::X:X
no ipv6 mld ssm-map static WORD X:X::X:X
no ipv6 mld (vrf NAME|) ssm-map static WORD X:X::X:X
```

Parameters

`vrf`	Specify the VRF name.
`WORD`	Specify IPv6 named standard access-list.
`X:X::X:X`	Specify IPv6 address.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to configure an SSM static mapping for group-address ff0e::1/128.

```
#configure terminal
(config)#ipv6 mld ssm-map static v6grp 2006::3
(config)#ipv6 access-list v6grp permit ff0e::1/128
```

ipv6 mld static-group

Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to MLD operation on a specific interface to statically add group and/or source records.

Use the `no` parameter with this command to delete static group membership entries.

Command Syntax

```
ipv6 mld static-group X:X::X:X {(source (X:X::X:X|ssm-map)|) (interface IFNAME|)}
no ipv6 mld static-group X:X::X:X {(source (X:X::X:X|ssm-map)|) (interface
  IFNAME|)}
```

Parameters

`X:X::X:X`	Standard IPv6 Multicast group address to be configured as a static group member.
`interface`	Physical interface. If used, static configuration is applied to the physical interface. If not used, static configuration is applied on all VLAN constituent interfaces.
`IFNAME`	Physical interface name.
`source`	Static source to be joined.
`X:X::X:X`	Standard IPv6 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 MLDv1 groups to translate these (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples shows how to statically add group and/or source records:

```
#configure terminal
(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10

(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10 source fe80::2fd:6cff:fe1c:b

(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10 source ssm-map
(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10 interface eth0
```

ipv6 mld version

Use this command to set the current MLD protocol version on an interface. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default version on an interface.

Command Syntax

```
ipv6 mld version <1-2>
no ipv6 mld version
```

Parameter

`<1-2>`	Specify a MLD protocol version number.

Default

Default MLD protocol version number is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld version 1
```

show debugging ipv6 mld

Use this command to display debugging information for MLD.

Command Syntax

```
show debugging ipv6 mld
show debugging ipv6 mld (vrf NAME|)
```

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output of the `show debugging mld` command:

```
#show debugging ipv6 mld
MLD Debugging status:
  MLD Decoder debugging is off
  MLD Encoder debugging is off
  MLD Events debugging is off
  MLD FSM debugging is off
  MLD Tree-Info-Base (TIB) debugging is off
#
```

show ipv6 mld groups

Use this command to display the multicast groups with receivers directly connected to the router, and learned through MLD.

Command Syntax

```
show ipv6 mld groups (detail|)
show ipv6 mld groups IFNAME (detail|)
show ipv6 mld groups IFNAME X:X::X:X (detail|)
show ipv6 mld groups X:X::X:X (detail|)
show ipv6 mld (vrf NAME|) groups (detail|)
show ipv6 mld (vrf NAME|) groups IFNAME (detail|)
show ipv6 mld (vrf NAME|) groups IFNAME X:X::X:X (detail|)
show ipv6 mld (vrf NAME|) groups X:X::X:X (detail|)
```

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`X:X::X:X`	Displays the multicast group address.
`IFNAME`	Interface name for which to display local information.
`detail`	MLDv2 source information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays local-membership information for all interfaces:

```
#show ipv6 mld groups
MLD Connected Group Membership
Group Address    Interface     Uptime      Expires    Last Reporter
ff1e::10         ge10          00:03:16    00:01:09   fe80::202:b3ff:fef0:79d8
```

Table 3-170: Show ipv6 mld groups

Entry	Description
Group Address	As stated.
Interface	A directly connected interface to the router
Uptime	Up time for multicast group

Table 3-170: Show ipv6 mld groups (Continued)

Entry	Description
Expires	Time before multicast group needs to send another uptime message to the directly connected router.
Last Reporter	IPv6 IP address of last reporte node in the group.

show ipv6 mld interface

Use this command to display the state of MLD, MLD Proxy service, and for a specified interface, or all interfaces.

Command Syntax

```
show ipv6 mld interface (IFNAME|)
show ipv6 mld (vrf NAME|) interface (IFNAME|)
```

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`IFNAME`	Interface name for which to display local information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following displays MLD interface status on all interfaces enabled for MLD.

```
#show ipv6 mld interface
Interface eth1 (Index 2)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::2fd:6cff:fe1c:b
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 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
#
```

Table 3-171: Show ipv6 mld interface output

Entry	Description
Interface	The type and name of the interface. (eth1, xe3/1, ge3, etc.).
MLD Enabled	Whether MLD is enabled on the interface.
Internet address	IPv6 internet address.
MLD interface	Number of group-record states.
MLD activity	MLD activity of the interface. In the example above, there is no activity.
MLD query interval	The amount of time between MLD queries.

Table 3-171: Show ipv6 mld interface output (Continued)

Entry	Description
MLD query timeout	The amount of time before the interface resends an MLD query.
MLD max query response time	The amount of time before the interface is considered no longer a multicast listener and is removed from the multicast.
Last member query response interval	The time in which if no query requests are received by the router, it assumes the multicast is over.
Group membership interval	The amount of time the router will wait for a group query before the group is considered gone.

show ipv6 mld ssm-map

Use this command to display MLD SSM (source-specific-multicast) mapping.

Command Syntax

```
show ipv6 mld ssm-map
show ipv6 mld ssm-map X:X::X:X
show ipv6 mld (vrf NAME|) ssm-map X:X::X:X
```

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`X:X::X:X`	Displays the multicast group address.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an example of this command:

```
#show ipv6 mld ssm-map
SSM Mapping : Enabled
Database    : None configured

#
```

CHAPTER 4 L2 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. By default report suppression is enabled.

Use the `no` parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping report-suppression
no igmp snooping report-suppression
```

Default

By default, report suppression is enabled.

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

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#sh 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 enabled
IGMPv3 Report suppression enabled
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 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 enabled
IGMPv3 Report suppression enabled
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 learned 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 4-172: 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 4-172: 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
```

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 state-refresh origination-interval
- ip pim unicast-bsm
- show debugging ip pim
- show debugging pim
- show ip pim bsr-router
- show ip pim interface
- show ip pim local-members
- show ip pim mroute
- show ip pim neighbor
- show ip pim nexthop
- 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 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, Virtual Routing (VR), and 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 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 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 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 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 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 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 (vrf NAME|) rp-address A.B.C.D (override|)
ip pim (vrf NAME|) rp-address A.B.C.D WORD (override|)
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

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	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
```

ip pim rp-candidate

Use this command to give the router a candidate RP status using the IP address of the specified interface.

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

```
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 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 1-173: 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 1-173: 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 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 1-174: 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 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 1-175: 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 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 1-176: 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 1-177: 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 1-177: 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 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 1-178: 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 1-179: 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 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
- snmp restart pim
- 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 2-180 explains the fields for each pim entry.

Table 2-180: 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 2-181 explains the fields for each pim entry.

Table 2-181: 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 2-181: (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 2-182 explains the fields for each pim entry.

Table 2-182: 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 2-183 explains the fields for each pim entry.

Table 2-183: 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.

Table 2-183: show ipv6 pim bsr-router

Entry	Description
Role	AS stated..
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 2-184 explains the fields for each pim entry.

Table 2-184: 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 2-185 explains the fields for each pim entry.

Table 2-185: 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 7 # Quality of Service

Quality of Service Configuration Guide

Contents

This document contains these chapters.

CHAPTER 1 QoS Introduction

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 behavior is an individual device's behavior 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 behavior.

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. IP traffic is classified using IP standard or IP extended ACLs. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS, but it is possible to match IP options against configured IP extended ACLs to enforce QoS.

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. Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN. Other frame types cannot carry Layer-2 CoS values. CoS values range from zero to seven, seven being the highest priority.

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. The process generates an internal DSCP for a packet, which identifies all future QoS actions to be taken on the packet. Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the DSCP is determined based on ACLs or the configuration. The Layer-2 CoS value is then mapped to a DSCP value. The classification is carried in the IP packet header using 6 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer-2 frame. 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, but not at the switch virtual interface level. Classification can be based on QoS ACLs, or class maps and policy maps.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal DSCP to the configured policer. 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.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, multiple classes of traffic across policy map share the aggregate policer.

Policing and policers have the following attributes:

- Policers can occur only on a physical port basis.
- Policing can occur on ingress interfaces.
- Only one policer can be applied to a packet per direction.

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 CoS queue. Each egress port can accommodate up 8 CoS 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 CoS priority is also obtained from the filtering mechanism result. After the packets are mapped to a CoS queue, they are scheduled.

Bandwidth Reservation

Bandwidth reservation is the minimum guaranteed bandwidth allocated per queue. Total guaranteed bandwidth of all the queues belonging to a particular port should not exceed the interface Bandwidth. In case if no Bandwidth reservation is done for the queue, minimum guaranteed per each queue will be 1% of the parent node [scheduling node or interface]

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
- Weighted Round Robin (WRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.The weights assigned for the queues will be in the ratio of bandwidth reservation of those queues
- Combination of WRR and SP, the Remaining Bandwidth will be scheduled in the strict order for the SP Queues. The Remaining Bandwidth will be scheduled in the WRR mode for WRR 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 DSCP values

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.

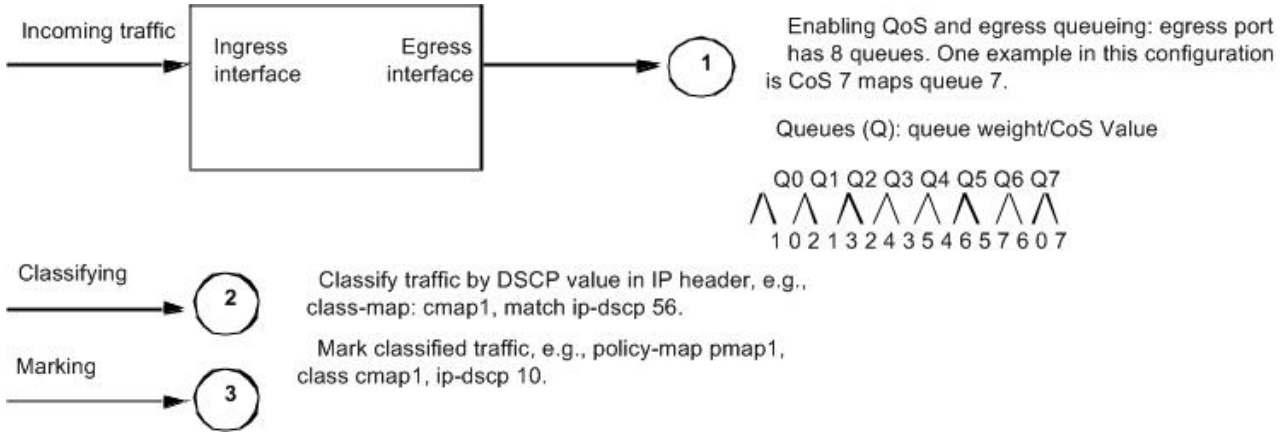
Policy Map

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 multiple class statements, 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.



Enable/Disable Configuration

Topology

Figure 1-26: Simple configuration of QoS

Enabling QoS

The following steps describe how to enable QoS.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
```

Disabling QoS

The following steps disable QoS.

`#configure terminal`	Enter configure mode.
`(config)#qos disable`	Disable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
% QoS is not enabled globally
```

QoS Statistics Configuration

This section show how to enable QoS statistics.

Topology

Figure 1-27: Simple configuration of QoS

Enabling QoS Statistics

The following steps describe how to enable QoS Statistics.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
```

CHAPTER 2 DSCP to Queue Map Configuration

This chapter contains a complete sample of configuring DSCP to queue map.

Topology

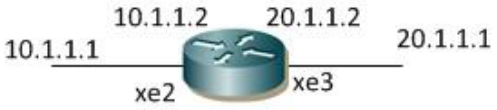


Figure 2-28: Simple configuration of DSCP to queue map

Configuration of DSCP to Queue Map on configuration mode

The following steps describe how to configure DSCP to queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos map dscp 10 queue 5`	Map DSCP 10 to queue 5 on global mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos map dscp 10 queue 5
qos statistics
!
```

Configuration of DSCP to Queue Map on Interface mode

The following steps describe how to configure DSCP to queue map on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#qos map dscp 10 queue 6`	Map DSCP 10 to queue 6 for all the unicast frames/ packets received on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
interface xe2
 qos map dscp 10 queue 6
!
```

CHAPTER 3 CoS to Queue Map Configuration

This chapter contains a complete sample of configuring CoS to queue map.

Topology

Figure 3-29: Simple configuration of CoS

Configuration of CoS to Queue Map on configuration mode

The following steps describe how to configure CoS to queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos map cos 2 queue 4`	Map CoS 2 to queue 4 on global mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
qos map cos 2 queue 4
!
```

Configuration of CoS to Queue Map on Interface mode

The following steps describe how to configure CoS to queue map on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#qos map cos 2 queue 4`	Map Cos 2 to queue 4 for all the unicast frames/packets received on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
interface xe2
 qos map cos 2 queue 4
!
```

CHAPTER 4 Trust DSCP on Layer 2 Interface Configuration

This chapter contains a complete sample of configuring trust DSCP on Layer 2 interface.

Topology

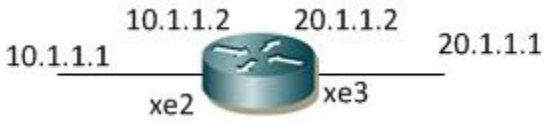


Figure 4-30: Simple configuration of trust DSCP

Configuration Trust DSCP on Interface mode

The following steps describe how to configure trust DSCP on Layer 2 interface.By default, Layer 2 interface will be trust CoS and layer3 interface will be trust DSCP.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#trust dscp`	Configure trust DSCP on the interface xe2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
!
interface xe2
 trust dscp
```

CHAPTER 5 Weights for Queues Configuration

This chapter contains a complete sample of configuring WRR weights for queues.

Topology

Figure 5-31: Simple configuration of QoS

Configuring WRR Weights for Queues

Do the following to configure WRR weights for queues.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map cmap1`	Enter class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as cos 2
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map cmap2`	Enter class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap1`	Assign class cmap1.
`(config-pmap-c-qos)#set qos-group 1`	Remark matched traffic to qos-group 1
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap2`	Assign class cmap2.
`(config-pmap-c-qos)#set qos-group 2`	Remark matched traffic to qos-group 2
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#class-map type queuing cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode.
`(config)#class-map type queuing cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode.
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2.
`(config-cmap-que)#exit`	Exit out of class-map mode.

(config)#policy-map type queuing pq1	Configure policy-map of type queuing with name pq1, and enter into policy-map mode.
(config-pmap-que)#class cq1	Attach class cq1 to Policy-map pq1.
(config-pmap-c-que)#wrr-queue weight 2	Configure WRR Weight of 2.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#class cq2	Assign class (queue) cq2 to pq1.
(config-pmap-c-que)#wrr-queue weight 4	Configure WRR weight of 4.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#exit	Exit from pmap mode.
(config)#interface xe2	Enter into interface xe2.
(config-if)#service-policy type queuing output pq1	Assign service policy pq1 of type queueing on out direction.
(config-if)#exit	Exit interface mode
(config)#exit	Exit configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)# service-policy type qos input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
```

```
!
class-map cmap1
 match cos 2
!
class-map cmap2
 match cos 3
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
 match qos-group 2
!
policy-map pmap1
 class cmap1
  set qos-group 1
  exit
 class cmap2
  set qos-group 2
  exit
!
!
policy-map type queuing pq1
 class type queuing cq1
  wrr-queue weight 2
  exit
 class type queuing cq2
  wrr-queue weight 4
  exit
!
!
interface xe2
 service-policy type queuing output pq1
!
interface xe3
 service-policy type qos input pmap1
!


#show policy-map

Type qos policy-maps
====================

policy-map pmap1
 class cmap1
  set qos-group 1
  exit
 class cmap2
  set qos-group 2
```

```
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit

policy-map type queuing pq1
 class type queuing cq1
  wrr-queue weight 2
  exit
 class type queuing cq2
  wrr-queue weight 4
  exit


#show class-map

  Type qos class-maps
  ===================
      class-map type qos match-any class-default

      class-map cmap1
         match cos 2
```

```
      class-map cmap2
         match cos 3


  Type queuing class-maps
  =======================
      class-map type queuing match-any cq1
         match qos-group 1

      class-map type queuing match-any cq2
         match qos-group 2

      class-map match-any q0

      class-map match-any q1

      class-map match-any q2

      class-map match-any q3

      class-map match-any q4

      class-map match-any q5

      class-map match-any q6

      class-map match-any q7


  Type Vlan-Queuing class-maps
  ============================

#show policy-map interface xe2
Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: pq1
---------------------------------
Class-map (queuing): cq1
 match qos-group 1
 wrr-queue weight 2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq2
 match qos-group 2
 wrr-queue weight 4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): cmap1 (match all)
 match cos 2
 set qos-group 1
      matched      : 209681694 packets, 15097081968 bytes
      transmitted  : 209681694 packets, 15097081968 bytes

Class-map (qos): cmap2 (match all)
 match cos 3
 set qos-group 2
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes
```

```
Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 11789 packets, 754820 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 1460 packets, 93914 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 39311112 packets, 2830400048 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q2
      output       : 78930334 packets, 5051541376 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 21 packets, 1428 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 6 Marking/Remarking Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

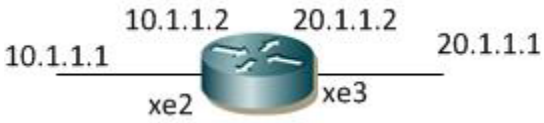


Figure 6-32: Simple configuration of Marking/Remarking

L2 Interface

The following steps describe how to configure Marking/Remarking.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 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 all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos cmap1`	Enter Class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as CoS with Value 2
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos pmap1`	Enter policy-map mode
`(config-pmap-qos)#class type qos cmap1`	Assign Class cmap1 to Policy-map pmap1
`(config-pmap-c-qos)#set cos 5`	Remark cos from cos 2 to cos 5
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe2 interface
`(config-if)#service-policy type qos input pmap1`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit the xe2 interface mode.

(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#class-map type qos cmap2	Enter Class-map mode
(config-cmap-qos)#match protocol arp	Configure match criteria as protocol with arp
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos pmap2	Enter policy-map mode
(config-pmap-qos)#class type qos cmap2	Assign Class cmap2 to Policy-map pmap2
(config-pmap-c-qos)#set cos 6	Remark all frame with ethertype as arp to cos 6
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap2	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.

(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos cmap1
 match cos 2
!
class-map type qos cmap2
 match protocol arp
!
policy-map type qos pmap1
 class type qos cmap1
  set cos 5
  exit
!
policy-map type qos pmap2
 class type qos cmap2
  set cos 6
  exit
!
!
!
interface xe2
 service-policy type qos input pmap1
!
interface xe3
 service-policy type qos input pmap2
!
```

```
#show class-map cmap1

  Type qos class-maps
  ===================

      class-map type qos cmap1
         match cos 2
```

```
#show policy-map
```

```
Type qos policy-maps
====================

policy-map type qos pmap1
 class type qos cmap1
  set cos 5
  exit

policy-map type qos pmap2
 class type qos cmap2
  set cos 6
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit


#show policy-map interface xe2

Interface xe2
Global statistics status : enabled
```

```
Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): cmap1 (match all)
 match cos 2
 set cos 5
      matched      : 8 packets, 680 bytes
      transmitted  : 8 packets, 680 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 12 packets, 1416 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
```

```
      output       : 589 packets, 37876 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q6
      output       : 7 packets, 448 bytes
      dropped      : 0 packets, 0 bytes

 Class-map (queuing): mc-q7
      output       : 12 packets, 852 bytes
      dropped      : 0 packets, 0 bytes

 Wred Drop Statistics :
 ----------------------
  green  : 0 packets
  yellow : 0 packets
  red    : 0 packets


 OcNOS#show policy-map interface xe3

 Interface xe3
 Global statistics status : enabled

 Service-policy (qos) input     : pmap2
 --------------------------------
```

```
Class-map (qos): cmap2 (match all)
 match protocol arp
 set cos 6
      matched      : 7 packets, 448 bytes
      transmitted  : 7 packets, 448 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 699 packets, 59550 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 2 packets, 136 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

L3 Interface

`#configure terminal`	Enter configure mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Assign IP Address on interface to 10.1.1.2 with mask 255.255.255.0
`(config-if)#exit`	Exit out of interface mode

(config)#qos enable	Enable QoS globally.
(config)#qos statistics	Enable QoS statistics.
(config)#class-map type qos cmap3	Configure class-map of type qos with name cmap3 and enter into Class-map mode
(config-cmap-qos)#match dscp 10	Configure match criteria as dscp with a value of 10.
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos pmap3	Enter policy-map mode
(config-pmap-qos)#class type qos cmap3	Assign Class cmap3 to Policy-map pmap3
(config-pmap-c-qos)#set dscp ef	Remark frames with dscp value 10 to dscp 46
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap3	Assign service-policy pmap3 to interface xe3 on in-direction
(config-if)#exit	Exit out of interface mode
(config)#ip access-list 101	Configure access-list 101 with action as permit for tcp traffic with destination port as ftp port
(config-ip-acl)#permit tcp any any eq ftp	Permit for tcp traffic with destination port as ftp port.
(config-ip-acl)#exit	Exit access list mode
(config)#class-map type qos match-any cmap4	Enter Class-map mode
(config-cmap-qos)#match access-group 101	Configure access-group 101 as match criteria
(config-cmap-qos)#exit	Exit class-map mode
(config)#policy-map type qos pmap4	Enter policy map mode
(config-pmap-qos)#class cmap4	Assign Class cmap4 to Policy-map pmap4
(config-pmap-c-qos)#set precedence 7	Remark frames matching access-group 101 to precedence 7
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.1/24	Assign IP Address on interface to 20.1.1.1 with mask 255.255.255.0
(config-if)#service-policy type qos input pmap4	Assign service-policy to interface on in-direction

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos cmap3
 match dscp af11
!
class-map type qos match-any cmap4
 match access-group 101
!
policy-map type qos pmap3
 class type qos cmap3
  set dscp ef
  exit
policy-map type qos pmap4
 class type qos cmap4
  set precedence network
  exit
!
interface xe2
 service-policy type qos input pmap4
!
interface xe3
 service-policy type qos input pmap3


#show class-map type qos

  Type qos class-maps
  ===================
      class-map type qos match-any class-default

      class-map type qos cmap3
         match dscp af11

      class-map type qos match-any cmap4
         match access-group 101



#show policy-map

Type qos policy-maps
====================

policy-map type qos pmap3
```

```
 class type qos cmap3
  set dscp ef
  exit

policy-map type qos pmap4
 class type qos cmap4
  set precedence network
  exit



#show policy-map interface xe2


Interface xe2
Global statistics status : enabled




Service-policy (qos) input     : pmap4
---------------------------------
 Class-map (qos): cmap4 (match any)
 match access-group 101
 set precedence 7
      matched    : 375594046 packets, 25540397168 bytes




Service-policy (queuing) output: default-out-policy
---------------------------------
 Class-map (queuing): q0
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

```
 Class-map (queuing): q3
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority level 1
      output     : 391282612 packets, 25042086656 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority level 1
      output     : 4 packets, 256 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show policy-map interface xe3


Interface xe3
Global statistics status : enabled


Service-policy (qos) input     : pmap3
--------------------------------
 Class-map (qos): cmap3 (match all)
 match dscp af11
 set dscp 46
      matched    : 401497149 packets, 25695819008 bytes


Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
```

```
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority level 1
      output     : 382211720 packets, 25990396484 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 7 Policing Configuration

Topology

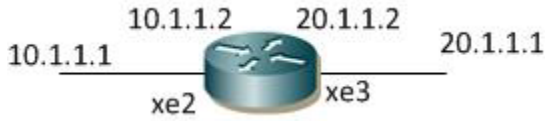


Figure 7-33: Simple configuration of Policing

L2 Interface

Do the following to configure policing on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as mstp aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 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 all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos 1234`	Enter Class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as CoS with Value 3
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos 1234`	Enter policy-map mode
`(config-pmap-qos)#class type qos 1234`	Assign Class 1234 to Policy-map 1234
`(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop`	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbyte, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR then Set the class of service (CoS) field to 1, if traffic violate the action then drop the frames.
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe2 interface
`(config-if)#service-policy type qos input 1234`	Assign service-policy to interface on in-direction
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 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 all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#mac access-list 102	Configure mac access-list with action
(config-mac-acl)#permit host 0000.0101.1010 host 0000.0202.2020	Permit when frames matches Source mac address 00:00:01:01:10:10 and destination mac address 00:00:02:02:20:20
(config-mac-acl)#exit	Exit mac access-list mode
(config)#class-map type qos match-any 2345	Enter Class-map mode
(cmap-qos-match-any-mode)#match access-group 102	Configure match criteria as access-group 102
(cmap-qos-match-any-mode)#exit	Exit Class-map mode
(config)#policy-map type qos 2345	Enter policy-map mode
(config-pmap-qos)#class type qos 2345	Assign Class 2345 to Policy-map 2345
(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbytes, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR, then set the class of service (CoS) field to 1, if traffic violate the action, then drop the frames.
(config-pmap-qos)#exit	Exit Policy-map mode
(config)#interface xe3	Enter interface mode.
(config-if)#service-policy type qos input 2345	Assign service-policy 2345 to interface on in-direction
(config-if)#exit	Exit interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos 1234
 match cos 2
!
class-map type qos match-any 2345
 match access-group 102
!
policy-map type qos 1234
 class type qos 1234
  police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5 violate
drop
  exit
policy-map type qos 2345
 class type qos 2345
```

```
  police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform tran
smit exceed set-cos-transmit 1 violate drop
  exit
!
interface xe2
 service-policy type qos input 1234
!
interface xe3
 service-policy type qos input 2345
#show class-map type qos

  Type qos class-maps
  ===================
      class-map type qos 1234
         match cos 2

      class-map type qos match-any 2345
         match access-group 102

      class-map type qos match-any class-default

#show policy-map type qos

Type qos policy-maps
====================

policy-map type qos 1234
 class type qos 1234
  police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5 violate
drop
  exit

policy-map type qos 2345
 class type qos 2345
  police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform tran
smit exceed set-cos-transmit 1 violate drop
  exit
#
#show policy-map interface xe2


Interface xe2
Global statistics status : enabled


Service-policy (qos) input     : 1234
--------------------------------
 Class-map (qos): 1234 (match all)
 match cos 2
 police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5 violate d
```

```
rop
      matched    : 7419394 packets, 504519132 bytes
      dropped    : 7409793 packets, 503866264 bytes


Service-policy (queuing) output: default-out-policy
---------------------------------
 Class-map (queuing): q0
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
      output     : 7222 packets, 491096 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority level 1
      output     : 14444 packets, 982192 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
```



```
 priority level 1
      output     : 2 packets, 246 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

```
#show policy-map interface xe3


Interface xe3
Global statistics status : enabled


Service-policy (qos) input     : 2345
--------------------------------
 Class-map (qos): 2345 (match any)
 match access-group 102
 police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform trans
mit exceed set-cos-transmit 1 violate drop
      matched    : 16218780 packets, 1102879420 bytes


Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```



```
 Class-map (queuing): q5
 priority level 1
      output     : 18527 packets, 1259836 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority level 1
      output     : 5 packets, 615 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
```

```
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 8 Bandwidth Configuration

This chapter contains a complete sample of configuring Bandwidth.

Topology

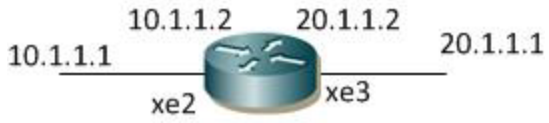


Figure 8-34: Simple configuration of Bandwidth

L2/L3 Interface

The following steps describe how to configure bandwidth.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to Policy-map P1
`(config-pmap-c-que)#bandwidth percent 70`	Configure minimum bandwidth as 70 percent of total bandwidth available on interface
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to Policy-map P1
`(config-pmap-c-que)#bandwidth percent 30`	Configure minimum bandwidth as 30 percent of remaining bandwidth available on interface after all allocations are done.
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode

(config)#class-map type qos c2	Enter Class-map mode
(config-cmap-qos)#match dscp 22	Configure match criteria as dscp 22
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policy-map mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 3 or dscp 10 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 4 or dscp 22 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos c1
 match dscp af11
 match cos 2
!
class-map type qos c2
 match dscp af23
 match cos 4
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
 match qos-group 2
!
policy-map type qos pmap1
 class type qos c1
  set qos-group 1
  exit
!
policy-map type queuing P1
 class type queuing cq1
  wrr-queue weight 1
  bandwidth percent 70
  exit
 class type queuing cq2
  wrr-queue weight 1
  bandwidth percent 30
  exit
!
!
!
interface xe2
 service-policy type queuing output P1
!
interface xe3
 service-policy type qos input pmap1
!


#show policy-map interface xe2
```

```
Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: P1
-----------------------------------
Class-map (queuing): cq1
 match qos-group 1
 wrr-queue weight 1
 bandwidth percent 70
      output       : 192415 packets, 13084220 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq2
 match qos-group 2
 wrr-queue weight 1
 bandwidth percent 30
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 191466 packets, 12253824 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 7048 packets, 451696 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 244636 packets, 16635248 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```



```
Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 1176 packets, 75608 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 16 packets, 1050 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

```
#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): c1 (match all)
 match dscp af11
 match cos 2
 set qos-group 1
      matched      : 173885 packets, 11824180 bytes
      transmitted  : 173885 packets, 11824180 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 12 packets, 1392 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
```



```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 1030 packets, 66126 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 5 packets, 346 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 9 Shaping Configuration

This chapter contains a complete sample of configuring Shaping.

Topology

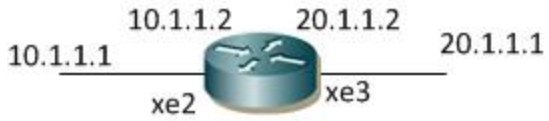


Figure 9-35: Simple configuration of Shaping

L2/L3 Interface

The following steps describe how to configure Shaping.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to Policy-map P1
`(config-pmap-c-que)#shape average 200 mbps`	Configure shaping to 200 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to Policy-map P1
`(config-pmap-c-que)#shape average 150 mbps`	Configure shaping to 150 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map type qos c2`	Enter Class-map mode
`(config-cmap-qos)#match dscp 22`	Configure match criteria as dscp 22

(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policy-map mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 3 or dscp 10 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 4 or dscp 22 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing

Type queuing policy-maps
========================

policy-map type queuing P1
 class type queuing cq1
  shape average 200 mbps
  wrr-queue weight 1
  exit
 class type queuing cq2
  shape average 150 mbps
  wrr-queue weight 1
  exit

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit


#show policy-map type qos
Type qos policy-maps
====================
```

```
policy-map type qos pmap1
  class type qos c1
    set qos-group 1
    exit
  class type qos c2
    set qos-group 2
    exit

#show class-map type queuing

  Type queuing class-maps
  =======================
      class-map type queuing match-any cq1
         match qos-group 1

      class-map type queuing match-any cq2
         match qos-group 2

      class-map match-any q0

      class-map match-any q1

      class-map match-any q2

      class-map match-any q3

      class-map match-any q4

      class-map match-any q5

      class-map match-any q6

      class-map match-any q7


#show class-map type qos
  Type qos class-maps
   ===================
           class-map type qos c2
                                match cos 4
                  match dscp 22

           class-map type qos c1
                                match cos 3
                  match dscp 10


#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
```

```
-------------------------------------------------------------------------------------
L0             L1             L2             Group  PrioLevel   Shape          Bandwidth
-------------------------------------------------------------------------------------
cq1                                             1      -           200 mbps       -
cq2                                             2      -           150 mbps       -


#show queuing interface xe3

Egress Queuing for Ethernet xe2 [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 policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
---------------------------------
Class-map (qos): c1 (match all)
 match dscp af11
 match cos 3
 set qos-group 1
      matched      : 371818 packets, 160915260 bytes
      transmitted  : 371818 packets, 160915260 bytes

Class-map (qos): c2 (match all)
 match dscp af23
 match cos 4
 set qos-group 2
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 122 packets, 7812 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
```



```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


OcNOS#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: P1
-----------------------------------
Class-map (queuing): cq1
 match qos-group 1
 shape average 200 mbps
 wrr-queue weight 1
      output       : 377827 packets, 163537138 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq2
 match qos-group 2
 shape average 150 mbps
 wrr-queue weight 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
```

```
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 6 packets, 708 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 6164 packets, 395284 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```



```
Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 21 packets, 1428 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 10 Weight Configuration

This chapter contains a complete sample of configuring weight.

Topology

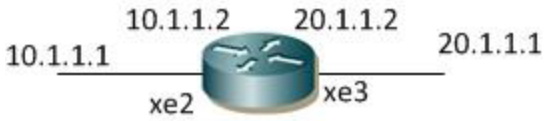


Figure 10-36: Simple configuration of Priority

ConfiguringL2 /L3 Interface

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default default-out-policy`	Enter policy-map type queueing default.
`(config-pmap-que-def)#class type queuing default q0`	Enter policy-class-map mode.
`(config-pmap-c-que-def)#wrr-queue weight 2`	Modify strict queue to wrr-queue with weight 2.
`(config-pmap-c-que-def)#exit`	Exit from policy-class-map mode.
`(config-pmap-que-def)#exit`	Exit from policy-map mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing  default default-out-policy
Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  wrr-queue weight 2
  bandwidth percent 1
  exit
 class type queuing default q1
  priority level 1
  bandwidth percent 1
  exit
 class type queuing default q2
  priority level 1
  bandwidth percent 1
  exit
 class type queuing default q3
```

```
 priority level 1
 bandwidth percent 1
 exit
class type queuing default q4
 priority level 1
 bandwidth percent 1
 exit
class type queuing default q5
 priority level 1
 bandwidth percent 1
 exit
class type queuing default q6
 priority level 1
 bandwidth percent 1
 exit
class type queuing default q7
 priority level 1
 bandwidth percent 1
 exit
```

```
#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
------------------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape          Bandwidth
------------------------------------------------------------------------------------------
q0                                              -      -           -              -
q1                                              -      High        -              -
q2                                              -      High        -              -
q3                                              -      High        -              -
q4                                              -      High        -              -
q5                                              -      High        -              -
q6                                              -      High        -              -
q7                                              -      High        -              -
#
```

CHAPTER 11 WRED Configuration

This chapter contains a complete sample of configuring WRED.

Topology

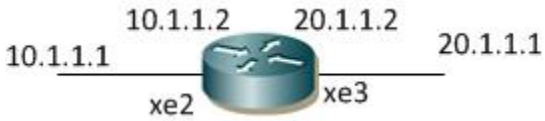


Figure 11-37: Simple configuration of WRED

L2/L3 Interface

The following steps describe how to configure WRED.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq3`	Configure class-map of type queuing with name cq3, and enter into class-map mode
`(config-cmap-que)#match qos-group 3`	Configure match criteria as qos-group 3
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to policy-map P1
`(config-pmap-c-que)#shape percent 20`	Configure shaping to 20 percent of bandwidth available on interface
`(config-pmap-c-que)#random-detect minimum-threshold 50 maximum-threshold 80 kbytes`	Configure WRED for minimum threshold of 50 kbytest and maximum threshold of 80 kbytes of queue size.
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to policy-map P1
`(config-pmap-c-que)#bandwidth 25000 kbps`	Configure bandwidth to 25000 kbps
`(config-pmap-c-que)#random-detect minimum-threshold 30 maximum-threshold 70 kbytes`	Configure WRED for minimum threshold of 30 kbytes and maximum threshold of 70 kbytes .
`(config-pmap-c-que)#exit`	Exit out of policy-class mode

(config-pmap-que)#class type queuing cq3	Attach class cq3 to policy-map P1
(config-pmap-c-que)# random-detect minimum-threshold 20 maximum-threshold 50 kbytes	Configure WRED for minimum threshold of 20 and maximum threshold of 50 kbytes.
(config-pmap-c-que)#bandwidth per 20	Configure bandwidth remaining for 20%
(config-pmap-que)#exit	Exit out of policy-map mode
(config)#class-map type qos c1	Enter Class-map mode
(config-cmap-qos)#match precedence 2	Configure match criteria as precedence 2
(config-cmap-qos)#match cos 2	Configure match criteria as cos 2
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter class-map mode
(config-cmap-qos)#match precedence 3	Configure match criteria as precedence 3
(config-cmap-qos)#match cos 3	Configure match criteria as cos 3
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c3	Enter Class-map mode
(config-cmap-qos)#match precedence 4	Configure match criteria as precedence 4
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policy-map mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 2 or precedence 2 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 3 or precedence 3 to qos-group 2
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#class type qos c3	Assign Class c3 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 3	Remark frames with either cos 4 or precedence 4 to qos-group 3
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#exit	Exit policy-map mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.

(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos c1
 match precedence immediate
 match cos 2
!
class-map type qos c2
 match precedence flash
 match cos 3
!
class-map type qos c3
 match precedence flashoverride
 match cos 4
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
```

```
 match qos-group 2
!
class-map type queuing match-any cq3
 match qos-group 3
!
policy-map type qos pmap1
 class type qos c1
  set qos-group 1
  exit
 class type qos c2
  set qos-group 2
  exit
 class type qos c3
  set qos-group 3
  exit
!
policy-map type queuing P1
 class type queuing cq1
  shape average percent 20
  wrr-queue weight 1
  random-detect minimum-threshold 50 maximum-threshold 80 kbytes
  exit
 class type queuing cq2
  wrr-queue weight 1
  random-detect minimum-threshold 30 maximum-threshold 70 kbytes
  bandwidth 25000 kbps
  exit
 class type queuing cq3
  wrr-queue weight 1
  random-detect minimum-threshold 20 maximum-threshold 50 kbytes
  exit
!
!
!
interface xe2
 service-policy type queuing output P1
!
interface xe3
 service-policy type qos input pmap1
!


#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: P1
-----------------------------------
Class-map (queuing): cq1
```

```
 match qos-group 1
 shape percent 20
 wrr-queue weight 1
 random-detect minimum-threshold 50 maximum-threshold 80 kbytes
percent
      output       : 814111 packets, 359980934 bytes
      dropped      : 3070548 packets, 1320403724 bytes

Class-map (queuing): cq2
 match qos-group 2
 wrr-queue weight 1
 random-detect minimum-threshold 30 maximum-threshold 70 kbytes
percent
 bandwidth 25000 kbps
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq3
 match qos-group 3
 wrr-queue weight 1
 random-detect minimum-threshold 20 maximum-threshold 50 kbytes
percent
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 59556244 packets, 25787484432 bytes
      dropped      : 2512 packets, 1103120 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 108 packets, 6912 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
```

```
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets



#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): c1 (match all)
 match precedence immediate
 match cos 2
 set qos-group 1
      matched      : 3718 packets, 1609160 bytes
      transmitted  : 3718 packets, 1609160 bytes

Class-map (qos): c2 (match all)
 match precedence flash
 match cos 3
 set qos-group 2
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): c3 (match all)
 match precedence flashoverride
 match cos 4
 set qos-group 3
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
---------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
```

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 99 packets, 6336 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
-------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
  Bandwidth
-------------------------------------------------------------------------------
cq1                                             1      -           20 percent
  -
cq2                                             2      -           -
  25000 kbps
cq3                                             3      -           -
  -


#show queuing interface xe1/2

Egress Queuing for Ethernet xe1/2 [System]
-------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
  Bandwidth
-------------------------------------------------------------------------------
q0                                              -      High        -
  -
q1                                              -      High        -
  -
q2                                              -      High        -
  -
q3                                              -      High        -
  -
q4                                              -      High        -
  -
q5                                              -      High        -
```

```
  -
q6                                          -       High        -
  -
q7                                          -       High        -
  -
```

CHAPTER 12 Tail-Drop Configuration

Topology

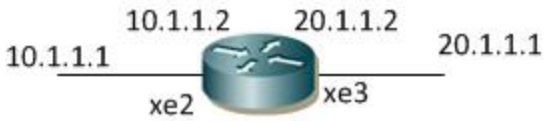


Figure 12-38: Simple configuration of Tail-Drop

Configuring Tail-Drop

The following steps describe how to configure Tail-Drop.

Configuration on L2/L3 Interfaces

Do the following to configure Tail-Drop on a queue.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq3`	Configure class-map of type queuing with name cq3, and enter into class-map mode
`(config-cmap-que)#match qos-group 3`	Configure match criteria as qos-group 3
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to policy-map P1
`(config-pmap-c-que)#shape percent 20`	Configure shaping to 20 percent of bandwidth available on interface
`(config-pmap-c-que)#queue-limit 100 packets`	Configure tail-drop for 100 packets
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to policy-map P1
`(config-pmap-c-que)#bandwidth 25000 kbps`	Configure bandwidth to 25000 kbps

(config-pmap-c-que)#queue-limit 99 packets	Configure tail-drop to 99 packets
(config-pmap-c-que)#exit	Exit out of policy-class mode
(config-pmap-que)#class type queuing cq3	Attach class cq3 to policy-map P1
(config-pmap-c-que)#queue-limit 101 packets	Configure tail-drop to 101 packets
(config-pmap-que)#exit	Exit out of policy-map mode
(config)#class-map type qos c1	Enter Class-map mode
(config-cmap-qos)#match precedence 2	Configure match criteria as precedence 2
(config-cmap-qos)#match cos 2	Configure match criteria as cos 2
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter Class-map mode
(config-cmap-qos)#match precedence 3	Configure match criteria as precedence 3
(config-cmap-qos)#match cos 3	Configure match criteria as cos 3
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c3	Enter Class-map mode
(config-cmap-qos)#match precedence 4	Configure match criteria as precedence 4
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policy-map mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 2 or precedence 2 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 3 or precedence 3 to qos-group 2
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#class type qos c3	Assign Class c3 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 3	Remark frames with either cos 4 or precedence 4 to qos-group 3
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#exit	Exit pmap mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.

(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos c1
 match precedence immediate
 match cos 2
!
class-map type qos c2
 match precedence flash
 match cos 3
!
class-map type qos c3
 match precedence flashoverride
 match cos 4
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
```

```
 match qos-group 2
!
class-map type queuing match-any cq3
 match qos-group 3
!
policy-map type qos pmap1
 class type qos c1
  set qos-group 1
  exit
 class type qos c2
  set qos-group 2
  exit
 class type qos c3
  set qos-group 3
  exit
!
policy-map type queuing P1
 class type queuing cq1
  shape average percent 20
  wrr-queue weight 1
  queue-limit 100 packets
  exit
 class type queuing cq2
  wrr-queue weight 1
  queue-limit 99 packets
  bandwidth 25000 kbps
  exit
 class type queuing cq3
  wrr-queue weight 1
  queue-limit 101 packets
  exit
!
!
!
interface xe1/1
 service-policy type queuing output P1
!
interface xe1/2
 service-policy type qos input pmap1
!

#show class-map

  Type qos class-maps
  ===================
      class-map type qos c1
         match cos 2
         match precedence immediate

      class-map type qos c2
```

```
        match cos 3
        match precedence flash

     class-map type qos c3
        match cos 4
        match precedence flashoverride

     class-map type qos match-any class-default


  Type queuing class-maps
  =======================
     class-map type queuing match-any cq1
        match qos-group 1

     class-map type queuing match-any cq2
        match qos-group 2

     class-map type queuing match-any cq3
        match qos-group 3

     class-map match-any q0

     class-map match-any q1

     class-map match-any q2

     class-map match-any q3

     class-map match-any q4

     class-map match-any q5

     class-map match-any q6

     class-map match-any q7


  Type Vlan-Queuing class-maps
  ============================


#show policy-map

Type qos policy-maps
====================

policy-map type qos pmap1
 class type qos c1
  set qos-group 1
```

```
  exit
 class type qos c2
  set qos-group 2
  exit
 class type qos c3
  set qos-group 3
  exit


Type queuing policy-maps
========================

policy-map type queuing P1
 class type queuing cq1
  shape average percent 20
  wrr-queue weight 1
  queue-limit 100 packets
  exit
 class type queuing cq2
  wrr-queue weight 1
  queue-limit 99 packets
  bandwidth 25000 kbps
  exit
 class type queuing cq3
  wrr-queue weight 1
  queue-limit 101 packets
  exit

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
```



```
 class type queuing default q7
  priority level 1
  exit


#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: P1
-----------------------------------
Class-map (queuing): cq1
 match qos-group 1
 shape percent 20
 wrr-queue weight 1
 queue-limit 100 packets
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq2
 match qos-group 2
 wrr-queue weight 1
 queue-limit 99 packets
 bandwidth 25000 kbps
      output       : 813899 packets, 351997930 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq3
 match qos-group 3
 wrr-queue weight 1
 queue-limit 101 packets
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 6 packets, 708 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 54378791 packets, 23548046696 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2401 packets, 153756 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 3 packets, 204 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): c1 (match all)
 match precedence immediate
 match cos 2
 set qos-group 1
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): c2 (match all)
 match precedence flash
 match cos 3
 set qos-group 2
      matched      : 833075 packets, 360302856 bytes
      transmitted  : 833075 packets, 360302856 bytes

Class-map (qos): c3 (match all)
 match precedence flashoverride
 match cos 4
 set qos-group 3
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 434 packets, 27788 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
```

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


OcNOS#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
  Bandwidth
------------------------------------------------------------------------------
cq1                                             1      -           20 percent
  -
cq2                                             2      -           -
  25000 kbps
cq3                                             3      -           -
  -
OcNOS#show queuing interface xe3

Egress Queuing for Ethernet xe3 [System]
------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
  Bandwidth
------------------------------------------------------------------------------
q0                                              -      High        -
  -
q1                                              -      High        -
  -
```

```
q2                                          -       High        -
  -
q3                                          -       High        -
  -
q4                                          -       High        -
  -
q5                                          -       High        -
  -
q6                                          -       High        -
  -
q7                                          -       High        -
  -
```

CHAPTER 13 FP Rules Queuing Configuration

This chapter contains basic information about cpu-queue properties and complete sample configuration for cpu-queue properties.

DUT has many CPU queues for management/classification of control traffic and provides rate limiters for control plane protection. Different types of CPU port bound packets are queued in different cpu-queues each with different properties like rate, queue-limit, monitoring status and drop status.

Topology

Figure 13-39: Simple configuration of CPU Queuing

Default Values

```
R1#show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status           Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow          -       32000          -       *lossy          -        monitor
bgp            -       1500           -        lossless       -        monitor
vrrp           -       500            -        lossless       -        monitor
ldp-rsvp       -       500            -        lossless       -        monitor
rip            -       500            -        lossless       -        monitor
ospf           -       2000           -        lossless       -        monitor
dhcp           -       100            -        lossy          -        no-
monitor
nd             -       6000           -        lossless       -        monitor
mpls           -       500            -        lossy          -        no-
monitor
pim            -       4000           -       *lossy          -       *no-
monitor
arp            -       6000           -        lossless       -        monitor
igmp           -       4000           -       *lossy          -       *no-
monitor
bpdu           -       10000          -        lossless       -        monitor
ccm            -       500            -        lossy          -        no-
monitor
bfd            -       2000           -        lossy          -        no-
monitor
ptp            -       1000           -        lossy          -        no-
monitor
isis           -       500            -        lossless       -        monitor
trill-isis     -       1000           -        lossless       -        monitor
acl            -       200            -       *lossy          -       *no-
monitor
vxlan          -       500            -        lossy          -        monitor
```

Note: Enable feature before validating cpu-queue for that protocol.

Monitor option will generate operational log, if it reaches above 90%. Log generation will stop, when it goes below 90%.

1. 2001 Jan 07 22:29:03.345 : R1 : HSL : NOTIF : [CPU_RATE_HIGH_4]: Average CPU queue rate for bpdu is 90% (540 pkts/sec).
2. 2001 Jan 07 22:29:08.346 : R1 : HSL : NOTIF : [CPU_QUEUE_RECOVERED_4]: CPU queue rate for bpdu is back to normal. Current average rate is 89%.

Lossless option will drop the traffic at ingress interface. We can use "show interface counters indiscard-stats" to verify the drop. Packets will be incremented in IBP Discards column.

Lossy option will drop the traffic at cpu. We can use “show interface cpu counters queue-stats`” to verify the drop.

“disable l3-protocols-cpu vxlan” command is used, when sending traffic to vxlan interface. In Vxlan, arp and nd traffic will go to vxlan queue. Remaining traffics are considered as data traffic.

Configuring CPU Queuing Lossless

Do the following to configure CPU queuing on an interface.

`#configure terminal`	
`(config)#bridge 1 protocol rstp`	Configure Bridge 1
`(config)#int xe52/2`	
`(config)#switchport`	Configure interface as L2
`(config-cmap-qos)#bridge-group 1`	Configure bridge 1 in interface
`(config-cmap-qos)#int xe52/3`	
`(config-cmap-qos)#switchport`	Configure interface as L2
`(config)#bridge-group 1`	Configure bridge 1 in interface
`(config-cmap-qos)#exit`	
`(config-cmap-qos)#cpu-queue bpdu rate 600 lossless no-monitor`	Configure bpdu cpu-queue with rate of 600 pps and lossless and no-monitor option

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
R1(config)#do show running-config | inc cpu
cpu-queue bpdu rate 600 lossless no-monitor
R1(config)#
R1(config)#do show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow         -       32000           -       *lossy          -        monitor
bgp           -       1500            -        lossless       -        monitor
```



```
vrrp          -       500             -       lossless       -       monitor
ldp-rsvp      -       500             -       lossless       -       monitor
rip           -       500             -       lossless       -       monitor
ospf          -       2000            -       lossless       -       monitor
dhcp          -       100             -       lossy          -       no-
monitor
nd            -       6000            -       lossless       -       monitor
mpls          -       500             -       lossy          -       no-
monitor
pim           -       4000            -      *lossy          -      *no-
monitor
arp           -       6000            -       lossless       -       monitor
igmp          -       4000            -      *lossy          -      *no-
monitor
bpdu      600         10000       lossless    lossless   no-monitor   monitor
ccm           -       500             -       lossy          -       no-
monitor
bfd           -       2000            -       lossy          -       no-
monitor
ptp           -       1000            -       lossy          -       no-
monitor
isis          -       500             -       lossless       -       monitor
trill-isis    -       1000            -       lossless       -       monitor
acl           -       200             -      *lossy          -      *no-
monitor
vxlan         -       500             -       lossy          -       monitor
R1(config)#do clear interface cpu counters
R1(config)#do clear interface counters

R1(config)#do show interface counters rate
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 po1                436           0            2980          5
 po2                768714        1372         769045        1373
 xe52/1             0             0            44            0
 xe52/2             0             0            263           0
 xe52/3             669424827     99971        263           0
 xe53/1             33            0            788           1
 xe53/2             33            0            719           1
 xe53/3             336           0            702           1
 xe53/4             33            0            769           1
 xe54/1             192176        343          192014        342
 xe54/2             192166        343          192292        343
 xe54/3             192150        343          192348        343
 xe54/4             192204        343          192390        343
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)  |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -             -            101679        1374
 bpdu         (100%) -             -            436856        600
```

```
 ospf          (  0%) -              -             84             0
 bgp           (  0%) -              -             44             0
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd        ( N/A) -              -             101574         1372
 bpdu          ( 99%) -              -             433465         599
 ospf          (  0%) -              -             39             0
 bgp           (  0%) -              -             44             0

R1(config)#do show interface cpu counters queue-sta
E - Egress, I - Ingress, Q-Size is in bytes
+---------------------+--------+----------------+------------------+---------
--------+--------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped
pkts   |   Dropped bytes   |
+---------------------+--------+----------------+------------------+---------
--------+--------------------+
hw-bfd           (E) 0       130582           9663068           0
0
bpdu            (E) 2706080  57086            41576707          0
0
arp              (E) 0       2                136               0
0
ospf             (E) 0       35               4658              0
0
bgp              (E) 0       95               7030              0
0


R1(config)#do show interface counters indiscard-stats
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+-------------+--------------------+
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy
Discards | EGR Port Unavail | IBP Discards |   Total Discards   |
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+-------------+--------------------+
 xe52/3       0                0              0              0
0                 13080579       13080579

Configuring cpu-queue with lossy
============================
```

Configuring CPU Queuing Lossy

Do the following to configure CPU queuing on an interface.

`#configure terminal`	
`R1(config)#cpu-queue  bpdu rate 500 lossy no-monitor`	Configure bpdu cpu-queue with rate of 500 pps and lossy and no-monitor option
`R1(config-if)#exit`	

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
R1(config)#do clear interface cpu counters
R1(config)#do clear interface  counters
R1(config)#do show running-config | inc cpu
cpu-queue bpdu rate 500 lossy no-monitor
disable l3-protocols-cpu vxlan
R1(config)#do show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow         -       32000           -       *lossy          -        monitor
bgp           -       1500            -        lossless       -        monitor
vrrp          -       500             -        lossless       -        monitor
ldp-rsvp      -       500             -        lossless       -        monitor
rip           -       500             -        lossless       -        monitor
ospf          -       2000            -        lossless       -        monitor
dhcp          -       100             -        lossy          -        no-
monitor
nd            -       6000            -        lossless       -        monitor
mpls          -       500             -        lossy          -        no-
monitor
pim           -       4000            -       *lossy          -       *no-
monitor
arp           -       6000            -        lossless       -        monitor
igmp          -       4000            -       *lossy          -       *no-
monitor
bpdu      500         10000       lossy        lossless   no-monitor   monitor
ccm           -       500             -        lossy          -        no-
monitor
bfd           -       2000            -        lossy          -        no-
monitor
ptp           -       1000            -        lossy          -        no-
monitor
isis          -       500             -        lossless       -        monitor
trill-isis    -       1000            -        lossless       -        monitor
acl           -       200             -       *lossy          -       *no-
monitor
vxlan         -       500             -        lossy          -        monitor
R1(config)#do show interface counters rate
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 po1                780           0            2974          5
 po2                769353        1373         769260        1373
 xe52/1             0             0            11            0
 xe52/2             0             0            248           0
 xe52/3             669564071     100000       248           0
```

```
 xe53/1              98             0             871            1
 xe53/2              98             0             692            1
 xe53/3              485            0             699            1
 xe53/4              98             0             710            1
 xe54/1              192647         343           192322         343
 xe54/2              191965         342           192280         343
 xe54/3              192466         343           192278         343
 xe54/4              192295         343           192416         343
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -              -             101505         1371
 bpdu         ( 99%) -              -             345547         499
 ospf         (  0%) -              -             74             0
 bgp          (  0%) -              -             44             0
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -              -             101505         1371
 bpdu         ( 99%) -              -             345547         499
 ospf         (  0%) -              -             74             0
 bgp          (  0%) -              -             44             0
R1(config)#do show cpu-queue details
cpu-queue bpdu rate 500 lossy no-monitor
disable l3-protocols-cpu vxlan
R1(config)#
R1(config)#
R1(config)#do 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   |
+--------------------+--------+-----------------+-------------------+---------
--------+--------------------+
hw-bfd           (E) 0       78216           5787984           0
0
bpdu            (E) 978848   39290           27124511          7818876
6550244016
arp              (E) 0       2               136               0
0
ospf             (E) 0       21              3070              0
0
bgp              (E) 0       55              4070              0
0

R1(config)#do show interface counters indiscard-stats
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+-------------+--------------------+
```

```
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy
Discards | EGR Port Unavail | IBP Discards |   Total Discards   |
+-------------+------------------+---------------+---------------+------------
-----+------------------+--------------+--------------------+
 xe53/3        4                  0               0               0
4                    0              4
 xe54/1        3                  0               0               0
3                    0              3
 xe54/2        2                  0               0               0
2                    0              2
 xe54/3        1                  0               0               0
1                    0              1
 xe54/4        3                  0               0               0
3                    0              3
```

CHAPTER 14 Explicit Congestion Notification (ECN) Configuration

Explicit congestion notification (ECN) enables end-to-end congestion notification between two endpoints on TCP/IP based networks. The two endpoints are an ECN-enabled sender and an ECN-enabled receiver. ECN must be enabled on both endpoints and on all of the intermediate devices between the endpoints for ECN to work properly. Any device in the transmission path that does not support ECN breaks the end-to-end ECN functionality.

WRED drops packets, based on the average queue length exceeding a specific threshold value, to indicate congestion. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED -- Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

ECN requires an ECN-specific field that has two bits--the ECN-capable Transport (ECT) bit and the CE (Congestion Experienced) bit--in the IP header. The ECT bit and the CE bit can be used to make four ECN field combinations of 00 to 11. The first number is the ECT bit and the second number is the CE bit. The table below lists each of the ECT and CE bit combination settings in the ECN field and what the combinations indicate.

Table 14-186 explains the output fields.

Table 14-186: show bfd fields

ECT Bit	CE Bit	Combination Indicates
0	0	Not- ECN capable
0	1	Endpoints of the transport protocol are ECN capable
1	0	Endpoints of the transport protocol
1	1	Congestion experienced

The ECN field combination 00 indicates that a packet is not using ECN. The ECN field combinations of 01 and 10 called as ECT(1) and ECT(0) respectively. This sets by the data sender to indicate that the endpoints of the transport protocol are ECN-capable. Routers treat those two field combinations identically. Data senders can use either one or both of these two combinations.

ECN is Enabled

If the number of packets in the queue is below the minimum threshold, packets are transmitted. This happens whether or not ECN is enabled, and this treatment is identical to the treatment a packet receives when WRED only is being used on the network.

If the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following three scenarios can occur:

If the ECN field on the packet indicates that the endpoints are ECN-capable (that is, the ECT bit is set to 1 and the CE bit is set to 0, or the ECT bit is set to 0 and the CE bit is set to 1)--and the WRED algorithm determines that the packet should have been dropped based on the drop probability--the ECT and CE bits for the packet are changed to 1, and the packet is transmitted. This happens because ECN is enabled and the packet gets marked instead of dropped.

If the ECN field on the packet indicates that neither endpoint is ECN-capable (that is, the ECT bit is set to 0 and the CE bit is set to 0), the packet might be dropped based on the WRED drop probability. This is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.

If the ECN field on the packet indicates that the network is experiencing congestion (that is, both the ECT bit and the CE bit are set to 1), the packet is transmitted. No further marking is required.

If the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Topology

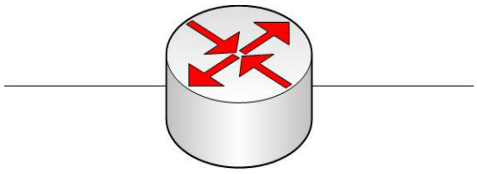


Figure 14-40: Simple configuration of ECN

Configuring ECN on L3 Interface

Do the following to configure ECN on anL3 interface.

`#configure terminal`	Enter inside configure mode
`(config)#qos enable`	Enable QoS on configuration mode.
`(config)#qos statisticsEnable`	QoS statistics on configuration mode.
`(config)#class-map match-any cmap`	Enter Class-map mode
`(cmap-qos-match-any-mode)#match precedence 3`	Configure match criteria as precedence with Value 3
`(config-pmap-qos)#policy-map pmap`	Enter policy-map mode
`(config-pmap-qos)#class cmap`	Assign Class cmap to Policy-map pmap
`(cmap-qos-match-any-mode)#match precedence 3`	Configure match criteria as precedence with Value 3
`(config-pmap-qos)#policy-map pmap`	Enter policy-map mode
`(config-pmap-qos)#class cmap`	Assign Class cmap to Policy-map pmap
`(config-pmap-c-qos)# police cir 328 mbps pir 556 mbps conform transmit exceed transmit violate transmit`	Police Precedence 3 frames @ Committed information rate of 328 mbps and pir 556 mbps conform transmit exceed transmit violate transmit.
`(config-pmap-c-qos)#end`	Exit out of policy-class-map mode
`#configure terminal`	Enter inside configure mode
`(config)#interface xe29`	Enter interface mode
`(config-if)#service-policy type qos input pmap`	Assign service-policy to interface on in-direction
`(config-if)#end`	Exit interface mode
`#configure terminal`	Enter inside configure mode
`(config)#policy-map type queuing default xyz`	Enter policy-map queuing mode

`(config-pmap-que-def)#class type queuing default q3`	Enter class-map type queuing
`(config-pmap-c-que-def)#shape percent 80`	Configure shape percent 80 in q3
`(config-pmap-c-que-def)# random-detect minimum-threshold 100 maximum-threshold 200 packets ecn`	Configure ECN with Random Early Detection which includes minimum and maximum threshold in packets
`#configure terminal`	Enter configure mode
`(config)#interface xe30`	Enter interface mode
`(config-if)#service-policy type queuing output xyz`	Attach policy on egress interface
`OcNOS(config-if)#end`	Exit configure mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
OcNOS#show policy-map interface xe30
Interface xe30
Global statistics status : enabled
Service-policy (queuing) output: xyz
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q3
 shape percent 80
 priority level 1
 random-detect minimum-threshold 100 maximum-threshold 200 packets ecn
      output       : 44808 packets, 67210500 bytes
      dropped      : 10516 packets, 15774000 bytes
Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q7
 priority level 1
```

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Wred Drop Statistics:
green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

Topology

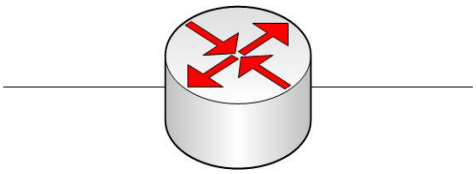


Figure 14-41: Simple configuration of ECN

Configuring ECN on L2 Interface

Do the following to configure ECN on anL2 interface.

`#configure terminal`	Enter inside configure mode
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP aware
`(config)#interface xe29`	Enter interface mode
`(config-if)#switchport`	Configure xe29 as a layer 2 port

(config-if)#bridge-group 1	Associate bridge to an interface
(config-if)#switchport mode trunk	Configure port as trunk
(config-if)#switchport trunk allowed vlan all	Allow all the vlan on the interface xe29
(config-if)#end	Exit the xe29 interface mode
#configure terminal	Enter inside configure mode
(config)#interface xe30	Enter interface mode
(config-if)#switchport	Configure xe30 as a layer 2 port
(config-if)#bridge-group 1	Associate bridge to an interface
(config-if)#switchport mode trunk	Configure port as trunk
(config-if)#switchport trunk allowed vlan all	Allow all the vlan on the interface xe30
(config-if)#end	Exit the xe30 interface mode
#configure terminal	Enter inside configure mode
(config)#qos enable	Enable QoS on configuration mode
(config)#qos statistics	Enable QoS statistics on configuration mode
(config)#class-map match-any cmap	Enter Class-map mode
(cmap-qos-match-any-mode)#match precedence 3	Configure match criteria as precedence with Value 3
(config-pmap-qos)#policy-map pmap	Enter policy-map mode
(config-pmap-qos)#class cmap	Assign Class cmap to Policy-map pmap
(config-pmap-c-qos)# police cir 328 mbps pir 556 mbps conform transmit exceed transmit violate transmit	Police Precedence 3 frames @ Committed information rate of 328 mbps and pir 556 mbps conform transmit exceed transmit violate transmit.
(config-pmap-c-qos)#end	Exit out of policy-class-map mode
#configure terminal	Enter inside configure mode
(config)#interface xe29	Enter interface mode
(config-if)#trust dscp	Configure trust DSCP on the interface xe29
(config-if)#service-policy type qos input pmap	Assign service-policy to interface on in-direction
(config-if)#end	Exit interface mode
#configure terminal	Enter inside configure mode
(config)#policy-map type queuing default xyz	Enter policy-map queuing mode
(config-pmap-que-def)#class type queuing default q3	Enter class-map type queuing
(config-pmap-c-que-def)#shape average 900 mbps	Configure shape average 900 in q3
(config-pmap-c-que-def)#random-detect green 1000 2000 yellow 3000 4000 red 5000 6000 bytes ecn	Configure ECN with Random Early Detection which includes minimum and maximum threshold for green, yellow and red packets
(config-pmap-c-que-def)#end	Exit pmap mode
#configure terminal	Enter configure mode
(config)#interface xe30	Enter interface mode
(config-if)#service-policy type queuing output xyz	Attach policy on egress interface
OcNOS(config-if)#end	Exit configure mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
 OcNOS#show policy-map interface xe30
Interface xe30
Global statistics status : enabled
Service-policy (queuing) output: xyz
----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q3
 shape average 900 mbps
 priority level 1
 random-detect green minimum-threshold 1000 maximum-threshold 2000 yellow
minimu
m-threshold 3000 maximum-threshold 4000 red minimum-threshold 5000 maximum-
thres
hold 6000 bytes ecn
      output       : 308318 packets, 462477000 bytes
      dropped      : 29774 packets, 44661000 bytes
Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q7
 priority level 1
      output       : 3 packets, 369 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
```



```
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

Quality of Service Command Reference

Contents

This document contains this chapter:

CHAPTER 1 Quality of Service Commands

This chapter is a reference for the ingress Quality of Service (QoS) and hierarchical QoS.

- set bridge dscp
- set cos
- set dscp
- set mpls class
- set precedence
- set qos-group
- set qos queue scheduler
- shape
- shape rate
- show class-map
- show cpu-queue details
- show policy-map
- show policy-map interface
- show queuing interface
- show running-config qos
- show running-config cpu-queue
- trust dscp
- wrr-queue weight

bandwidth

Use this command to allocate a minimum percentage of the interface bandwidth to a queue.

Use the `no` command to remove a bandwidth configuration.

Command Syntax

```
bandwidth (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
no bandwidth (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
```

Parameters

`<1-1000000000>`	Bandwidth value
`kbps`	Units in kilobits/sec.
`mbps`	Units in megabits/sec.
`gbps`	Units in gigabits/sec.
`percent`	Specify the percentage from 1 to 100.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing PQOS
(config-pmap-que)# class type queuing 1p7q4t-out-pq1
(config-pmap-c-que)# bandwidth 10 mbps
```

bandwidth remaining

Use this command to configure the bandwidth remaining on the interface in a queue.

Use the `no command` to remove the remaining bandwidth allocation.

Command Syntax

```
bandwidth remaining percent <1-100>
no bandwidth remaining percent <1-100>
```

Parameters

`<1-100>`	Specify the percentage of remaining bandwidth on the underlying link.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1
(config-pmap-que)#class type queuing q1
 (config-pmap-c-que)# bandwidth percent 70
(config-pmap-c-que)#exit
(config-pmap-que)#class type queuing q2
(config-pmap-c-que)# bandwidth remaining percent 30
```

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.

In a class-map, adding or deleting match criteria with misconfiguration will have silent exit and will not proceed with operation.

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 before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# class-map type qos C_QOS1
```

class-map type queuing

Use this command to create a class-map of type queuing.

Use the `no` command to remove a class-map.

Note: Class-maps with no action are treated as incomplete configuration and don't take any effect until the action is added. Class-map deletion is not allowed if it is referenced by any policy-map.

Command Syntax

```
class-map type queuing (match-any|) NAME
no class-map type queuing (match-any|) 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, class-map type is match-any

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
#configure terminal
(config)# class-map type queuing 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: Implicit priority of the classes in a policy-map will be calculated based number of matches with VLAN match given lower weight-age over other matches. In case of classes with conflicting match, it is not guarantied which class the traffic would hit. User is recommended to use priority in such cases.

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 before OcNOS version 1.3.

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.

Use the `no` command to remove a queuing class-map from the policy map.

Command Syntax

```
class (type queuing ((default (q0|q1|q2|q3|q4|q5|q6|q7))|NAME) | NAME | queuing
  class-default)
no class (type queuing|) NAME
```

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 before OcNOS version 1.3.

Examples

```
(config)#
(config)#policy-map type queuing PP
(config-pmap-que)#class type queuing C_PP_1
```

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 before OcNOS version 1.3.

Examples

```
#clear qos statistics
```

cpu-queue

Use this command to configure create a cpu queue for vxlan.

Use the no form of this command to remove a cpu queue.

Command Syntax

```
cpu-queue <queue-name> ( (rate <value>|)  (lossy|lossless|)  (monitor|no-monitor|)
  )
no cpu-queue <queue-name> ( (rate|)  (lossy|lossless|)  (monitor|no-monitor) |)
```

Parameters

`queue-name`	Name of the cpu queue
`rate`	When the packets are uplifted
`lossy`	If enabled, packets are dropped at cpu-queue when the cpu-queues congested
`loseless`	If enabled, packets are dropped at ingress port
`monitor`	Enable logging when cpu-queue discards packets
`no-monitor`	Disable logging

Default

Default value for vxlan cpu-queue command is 500.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#configure terminal
(config)#cpu-queue cpu 500
(config-dscp-queue)#exit
```

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

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 before OcNOS version 1.3.

Examples

```
(config)# class-map class_acl
(config-cmap-qos)# match access-group name 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 (not|) cos WORD
no match (not|) 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 before OcNOS version 1.3.

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 (not|) cos inner WORD
no match (not|) 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 before OcNOS version 1.3.

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`.

Command Syntax

```
match (not|) 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 (not|) 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 before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS7
(config-cmap-qos)#match dscp 48-55
```

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 (not|) ip rtp WORD
no match (not|) 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 before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match ip rtp 2300
```

match mac

Use this command to classify based on the mac address (can be source or destination or both)

Use the `no` command to remove the match configuration.

Command Syntax

```
match mac (src |dest ) (XX:XX:XX:XX:XX:XX| XX-XX-XX-XX-XX-XX |XXXX.XXXX.XXXX)
no match mac (src |dest ) (XX:XX:XX:XX:XX:XX| XX-XX-XX-XX-XX-XX |XXXX.XXXX.XXXX)
```

Parameters

`Mac`	Ethernet mac address
`Src`	specifies the source mac
`Dest`	specifies the destination mac
`XX:XX:XX:XX:XX:XX`	MAC address option 1
`XX-XX-XX-XX-XX-XX`	MAC address option 2
`XXXX.XXXX.XXXX`	MAC address option 3

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match mac src 11:22:33:44:55:66
(config-cmap-qos)#match mac dest 3344.5566.7788
```

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`.

Command Syntax

```
match (not|) precedence [WORD | critical | flash | flash-override | immediate |
  internet | network | priority | routine]
```

```
no match (not|) 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 before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)#  7
```

match protocol

Use this command to classify traffic based on protocol.

Use the `no command` to remove the specified protocol as a match criteria.

Command Syntax

```
match (not|) protocol (arp | bridging |cdp | clns | clns-is |clns-es | dhcp | isis
  | ldp| netbios )
no match (not|) protocol (arp|bridging|cdp|clns|clns-es| clns-is| dhcp |isis |ldp
  |netbios|all)
```

Parameters

`arp`	Address Resolution Protocol (ARP)
`bridging`	Bridging
`cdp`	Cisco Discovery Protocol (CDP)
`clns`	Connection-less Network Service (CLNS)
`clns-is`	CLNS Intermediate System
`clns-es`	CLNS end System
`dhcp`	Dynamic Host Configuration (DHCP)
`isis`	Intermediate system to intermediate system (IS-IS)
`ldp`	Label Distribution Protocol (LDP)
`netbios`	NetBIOS Extended User Interface (NetBEUI)
`all`	Delete all matched protocols.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match protocol ldp
```

match qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` to remove a QoS match on a queue number from a type queuing class map.

Command Syntax

```
match qos-group <1-2000>
no match qos-group <1-2000>
```

Parameters

`<1-2000>`	Specify qos group value or list of qos group values specified in bytes.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#class-map type queuing match-any C_PP_1
(config-cmap-que)#match qos-group 1
```

match traffic-type

Use this command to classify based on traffic-type

Use the `no` command to remove the match configuration.

Note: Class with match traffic type default will have lower priority over class with other traffic type match.

Command Syntax

```
match (not|) traffic-type (l2-uc|l2-uc-unknown|default)
no match (not|) traffic-type (l2-uc|l2-uc-unknown|default)
```

Parameters

`Traffic-type`	type of traffic to be matched
`l2-uc`	L2 Unicast traffic
`l2-uc-unknown`	Unknown L2 Unicast traffic
`default`	All other traffic-types

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match traffic-type l2-uc
```

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 (not|) vlan WORD
no match (not|) vlan (WORD|all)
```

Parameters

`not`	Match all except this.
`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 before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan 1
```

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 (not|) vlan inner WORD
no match (not|) vlan inner (WORD|all)
```

Parameters

`not`	Match all except this.
`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 before OcNOS version 1.3.

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 Peak Information Rate (PIR) can only be whole numbers.

Command Syntax

```
police (colour-blind | colour-aware|)(cir) (<1-2000000000> (kbps|mbps|gbps)) ((pir
  (<1-2000000000> (kbps|mbps|gbps))|)((bc) <1-256000>
  (kbytes|mbytes|ms|us)|)((be)<1-256000> (kbytes|mbytes|ms|us)|)((conform (transmit
  | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> |
  set-mpls-class <0-7> )) |)((exceed (drop | set-dscp-transmit <0-63> | set-cos-
  transmit <0-7> | transmit | set-mpls-class <0-7> ))|) ((violate (drop | set-dscp-
  transmit <0-63> | set-cos-transmit <0-7> | transmit | set-mpls-class <0-7> ))|))
no police (cir) (<1-2000000000> (kbps|mbps|gbps)) ((pir (<1-2000000000>
  (kbps|mbps|gbps))|)((bc) <1-256000> (kbytes|mbytes|ms|us)|)((be)<1-256000>
  (kbytes|mbytes|ms|us)|)((conform (transmit | set-prec-transmit <0-7> | set-dscp-
  transmit <0-63> | set-cos-transmit <0-7> | set-mpls-class <0-7> )) |)((exceed
  (drop | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit | set-mpls-
  class <0-7> ))|) ((violate (drop | set-dscp-transmit <0-63> | set-cos-transmit
  <0-7> | transmit | set-mpls-class <0-7> ))|))
```

Parameters

`colour-blind` Do not police on color.

`colour-aware` Do police on color.

`cir <1-2000000000>`

Specify Committed information rate.

`pir <1-2000000000>`

Peak 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 <1-256000>`

Burst rate committed.

`be <1-256000>` Burst rate extended.

`transmit` Specify the action of transmitting packets.

`set-prec-transmit`

Sets the IP precedence field to the specified value and transmits the packet.

`set-dscp-transmit`

Sets the Differentiated Service Code Point (DSCP) field to the specified value and transmits the packet.

`set-cos-transmit`

Sets the class of service (CoS) field to the specified value and transmits the packet.

`set-mpls-class`	
	Set the mpls class filed to the give value and tx the packet
`drop`	Specify the action of dropping packets.
`conform`	Sets the action to take when the data rate is within bounds
`exceed`	Sets the action to take when the data rate is exceeded. Default is drop.
`violate`	Sets the action to take when the data rate violates the configured rate values. The default is drop.

Default

Table 1-187: Default values

Parameter	Default
policer-type	Color-Blind
`cir`	N/A
`pir`	0
`bc`	0
`be`	0
`conform`	Transmit
`exceed`	Drop
`violate`	Drop

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# policy-map type qos 2345
(config-pmap-qos)#class type qos 2345
(config-pmap-c-qos)# police cir 2 mbps pir 4 mbps bc 2 mbytes be 4 mbytes conform
transmit exceed set-cos-transmit 1 violate drop
```

Usage

Traffic policing is based on the concept of *marking* IP packets, and then *metering* the packets in relation to how they are marked. This is called the “Two Rate Three Color Marker (trTCM)” process.

The Two Rate Three Color Marker (trTCM) meters an IP packet stream, and marks its packets as either green, yellow, or red. A packet is marked RED if it exceeds the *Peak Information Rate* (PIR). Otherwise it is marked either YELLOW or GREEN depending on whether it exceeds or does not exceed the Committed Information Rate (CIR). The trTCM is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

The Meter meters each packet and passes the packet and the metering result to the Marker. The Meter operates in one of two modes – Color-Blind or Color-Aware. In the Color-Blind mode, the Meter assumes that the packet stream is uncolored.In the Color-Aware mode, the Meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either GREEN, YELLOW, or RED.

The following describes the equations used to determine the BC an BE values:

Note: CIR, PIR, BC, and BE values are all in kbits/sec.

```
=================
BC = CIR * 5 / 1000;
Range check [64kbytes-256mbytes]
if (BC / 8) < 64)
then BC = 64 * 8;
else if (BC / 8) > 256000)
then BC = 256000 * 8;
=================
```

Same calculation for BE, as well.

Note: If the PIR value is not mentioned in the configuration, then the CIR value itself is considered for BE calculation.

```
=================
BE = PIR * 5 / 1000;
Range check [64kbytes-256mbytes]
if (BE / 8) < 64)
then BE = 64 * 8;
else if (BE / 8) > 256000)
then BE = 256000 * 8;
==================
```

For example:

```
Configure: police CIR 1 mbps
Hardware: CIR = 1000kbits/sec , BC = 512kbits, BE = 512kbits

Configure: police CIR 1 mbps PIR 200 mbps
Hardware: CIR = 1000kbits/sec, BC = 512kbits, PIR = 200000kbits/sec, BE = 1000kbits
```

For additional information regarding policing, see RFC 2697 and RFC 2698.

policy-map

Use this command to create a policy map and enter policy-map mode.

Use the `no` 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 before OcNOS version 1.3.

Examples

```
(config)#
(config)#policy-map type qos PQOS
```

priority

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 before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#priority 20
```

priority level

Use this command to configure a single output queuing class as the priority queue.

Note: Priority can be set only on default queues (such as queues in the default queuing policy-map).

Command Syntax

```
priority (level VALUE |)
```

Parameters

VALUE	Specify the priority level for an output queuing class. Only one priority level is supported. The priority value can only be 1.

Default

No default value is specified

Command Mode

Policy map-class type queuing mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

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 1
```

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 before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# qos enable

(config)#qos disable
```

qos map

Use this command to map either a Differentiated Services Control Protocol (DSCP) value or a Class of Service (CoS) value to a particular queue.

Use the no form of this command to remove the mapping.

Command Syntax

```
qos map ((cos <0-7> | dscp <0-63> ) | queue <0-7>))
no qos map ((cos <0-7> | dscp <0-63> ) | queue <0-7>))
```

Parameters

<0-7>	CoS value
<0-63>	DSCP value
<0-7>	Identifying queue number

Default

By default, CoS to queue mapping is one to one.

By default, 8 DSCP values are mapped to one queue. For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

Configure, Interface modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#qos map cos 1 queue 7

(config)#qos map dscp 45 queue 1
```

Example for one to one CoS to queue mapping:

```
(config)#qos map cos 1 queue 1

(config)#qos map cos 2 queue 2
```

qos remark dei

Use this command to enable remarking of the Drop Eligible Indicator (DEI) bit.

Use the `no` command to disable remarking of the DEI bit.

Command Syntax

```
qos remark dei
no qos remark dei
```

Parameters

None

Default

By default, remarking of the DEI bit is disabled.

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)#qos remark dei
(config)#
```

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 before OcNOS version 1.3.

Examples

```
(config)#qos statistics
(config)#
```

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 (<1-524288>) (packets | bytes | kbytes)
no queue-limit (<1-524288>) (packets | bytes | kbytes)
```

Parameters

`<1-524288>`	Specify queue-limit in packets, bytes, or Kilobytes. Max value for bytes is 524288 Max value for kilobytes is 512 Max value for packets is 600

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1
(config-pmap-que)#class type queuing q1
(config-pmap-c-que)# queue-limit percent 50
```

random-detect

Use this command to configure weighted random early detection (WRED).

Use the `no command` to remove a WRED configuration.

Note: Explicit Congestion Notification (ECN) ECN-WRED is independent of WRED and max queue size parameters. With ECN, queue size can be reached until default max queue size is exceeded.

Command Syntax

```
random-detect (green (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>
  yellow (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288> red
  (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>)(packets | bytes |
  kbytes)(ecn|)
no random-detect (green (minimum-threshold|)<1-524288> (maximum-threshold|)<1-
  524288> yellow (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>
  red(minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>)(packets | bytes
  |kbytes)(ecn|)
```

Parameters

`minimum-threshold`

Specify the minimum threshold. In the range of <1-524288>

`maximum-threshold`

Specify the maximum threshold. In the range of <1-524288>

`Packets, bytes, kbytes`

Specify the thresholds in Packets, Bytes, or Kilobytes.

`ecn` Explicit Congestion Notification

Default

No default value is specified

Command Mode

Policy-class map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, Trident III, Tomahawk, and Helix platforms.

Examples

```
(config)# policy-map type queuing default xyz
(config-pmap-que)#class type queuing default q1
(config-pmap-c-que)# random-detect minimum-threshold 200 maximum-threshold 512
kbytes ecn
```

service-policy

Use this command to attach a child policy onto a parent policy.

Use the `no` command detach child policy from the parent policy.

Command Syntax

```
service-policy NAME
no service-policy NAME
```

Parameters

`NAME`	Specify the policy map to attach to this interface.

Default

No default value is specified

Command Mode

Policy-class-map queuing mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#policy-map type queuing P1
(config-pmap-que)#class type queuing empty5b
(config-pmap-c-que)#service-policy PQOS
```

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|output) NAME
no service-policy type qos (input|output) 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 before OcNOS version 1.3.

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 before OcNOS version 1.3.

Examples

```
(config)#int xe3
(config-if)#service-policy type queuing output PQOS
```

set bridge cos

Use this command to set the Class-of-Service (CoS) value for L2 packets only.

Use the `no` parameter with this command to unset a CoS value.

Command Syntax

```
set bridge cos (<0-7>)
no set bridge cos <0-7>
```

Parameters

`<0-7>`	CoS value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge cos 2
```

set bridge dscp

Use this command to set the DSCP value for L2 packets only.

Use the `no` parameter with this command to unset a DSCP value.

Command Syntax

```
set bridge 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 bridge 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-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge dscp 25
```

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.

Command Syntax

```
set cos <0-7>
no set cos <0-7>
```

Parameters

`<0-7>`	Specify CoS value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

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 mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set dscp af12
```

set mpls class

Use this command to set mpls class(queue) for the matched packet.

Use the no command to remove the assigned value from the class.

Command Syntax

```
set mpls class <0-7>
no set mpls class <0-7>
```

Parameters

<0-7>	Specify class value to assign for this traffic.

Default

No default value is specified

Command Mode

Policy-map type qos

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# set mpls class 3
(config-pmap-c-qos)#
```

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 mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map policy1
(config-pmap-qos)# class class2
(config-pmap-c-qos)# set precedence 3
(config-pmap-c-qos)#
```

set qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` command to remove a QoS group match on a queue number from a type queuing class map.

Command Syntax

```
set qos-group <1-2000>
no set qos-group <1-2000>
```

Parameters

`<1-2000>`	Specify the QoS group value to assign for this class of traffic.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#policy-map type qos PQOS
(config-pmap-qos)#class type qos C_QOS1
(config-pmap-c-qos)#set qos-group 1
```

set qos queue scheduler

Use this command to change the scheduler mode of Unicast Queue and Non-Unicast queue groups to WRR or SP.

Use the `no` command to disable the set mode, and to change to the default mode

Command Syntax

```
set qos ((wrr uc <1-127> non-uc <1-127>)|(sp uc <0-1> non-uc <0-1>))
no set qos ((wrr uc <1-127> non-uc <1-127>)|(sp uc <0-1> non-uc <0-1>))
```

Parameters

wrr	Weighted Round Robin Mode
uc - <1-127>	Unicast Queues
non-uc <1-127>	Non-Unicast Queues
sp	Strict Priority Mode

Default

The default is WRR with 32:2.

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#set qos wrr uc 30 non-uc 40
(config)#
```

shape

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.

Command Syntax

```
shape (average|) (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
no shape (average|) (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
```

Parameters

`average`	Specify an optional keyword. Shaping is based on an average rate. Average rate for shaping in the range of `<1-1000000000>`
`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 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# policy-map type queuing my_queue
(config-pmap-que)# class type queuing PQOS
(config-pmap-c-que)# shape percent 25
(config-pmap-c-que)#
```

shape rate

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.

Command Syntax

```
shape rate <1-1000000000> (kbps|mbps|gbps) burst SHAPE_BURST_RATE
no shape rate
```

Parameters

`<1-1000000000>`	Average rate for shaping in the following range: 8 kbps to 1000 gbps for Trident3 1 kbps to 1000 gbps for other XGS platforms
`kbps`	Units of kbps per second.
`mbps`	Units of mbps per second.
`gbps`	Units of gbps per second.
`SHAPE_BURST_RATE`	Burst value in kbits in the following range: <2-1000000> for Trident3 <1-1000000> for other XGS platforms

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
(config)#interface xe11
(config-if)#shape rate 100 mbps burst 20
```

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 before OcNOS version 1.3.

Examples

```
#show class-map type qos
Type qos class-maps
===================
class-map type qos 1234
match cos 3
class-map type qos 2345
QOS-ACCESS-LIST-NAME: 101


#show class-map 1234
Type qos class-maps
===================
class-map type qos 1234
match cos 3
```

show cpu-queue details

Use this command to display details about CPU queue for QoS.

Command Syntax

```
show cpu-queue details
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========  ===========
sflow     10000       32000           -       *lossy      no-monitor   monitor
bgp           -       1500            -        lossless       -        monitor
vrrp          -       500             -        lossless       -        monitor
ldp-rsvp      -       500             -        lossless       -        monitor
rip           -       500             -        lossless       -        monitor
ospf      0           2000        lossy        lossless   monitor      monitor
dhcp          -       100             -        lossy          -        no-monitor
nd        200         6000        lossless     lossless   monitor      monitor
mpls          -       500             -        lossy          -        no-monitor
pim           -       4000            -       *lossy          -       *no-monitor
arp       100         6000        lossy        lossless   no-monitor   monitor
igmp          -       4000            -       *lossy          -       *no-monitor
bpdu      1000        10000           -        lossless   monitor      monitor
ccm           -       500             -        lossy          -        no-monitor
bfd           -       2000            -        lossy          -        no-monitor
ptp           -       1000            -        lossy          -        no-monitor
isis          -       500             -        lossless       -        monitor
trill-isis    -       1000            -        lossless       -        monitor
acl           -       200             -       *lossy          -       *no-monitor
```

```
    vxlan          -       500             -       lossy          -       monitor
```

Table 1-188 explains the output fields.

Table 1-188: show CPU Queue fields

Entry	Description
CPU queue name	Name of the CPU queue
Rate In PPS	At which packets are successfully delivered
`Lossy Status`	Status of the network lossy or lossless
`Monitor Status`	Status of the network monitor

show policy-map

Use this command to display qos/queuing policy-map.

Command Syntax

```
show policy-map (type (qos (statistics |)|queuing|vlan-queuing|hybrid-queuing)|)
show policy-map (type (qos (statistics |)|vlan-queuing|hybrid-queuing|queuing
  (default |))|) NAME
```

Parameters

`qos`	Specify the policy maps of the type qos only.
`statistics`	Displays QoS statistics.
`queuing`	Specify the policy maps of the type queuing only.
`default`	Default queue of the port
`NAME`	Specify named policy map.

Command Mode

Exec and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Examples

```
#show policy-map type qos statistics
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
|  Interface  |      Class-map     |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes  |
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
Policy-map: p5 (input)
xe3/1          c5                   213537882         14520578356       -                 -
Policy-map: q5 (input)
xe3/2          c5                   213538483         14520618816       -                 -

#show policy-map type qos statistics p5
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
|  Interface  |      Class-map     |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes  |
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
Policy-map: p5 (input)
xe3/1          c5                   246954616         16792916200       -                 -
```

show policy-map interface

Use this command to display the statistics and the configurations of the input and output policies that are attached to an interface.

Command Syntax

```
show policy-map interface (NAME (input | output | ) (type (qos | queuing)|) | brief)
```

Parameters

NAME	Interface name.
brief	brief policy interface.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show policy-map interface xe19/1


Interface xe19/1
Global statistics status : enabled

Service-policy (qos) input : p1
---------------------------------
 Class-map (qos): c1 (match all)
 match vlan 2
 police cir 2 mbps
      matched    : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (qos): c3 (match all)
 police cir 2 mbps
      matched    : 2172408 packets, 2172408000 bytes
      dropped    : 2128959 packets, 2128959000 bytes


Service-policy (queuing) output: default-out-policy
---------------------------------
 Class-map (queuing): q0
 priority level 1
 bandwidth percent 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
```

```
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q2
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q3
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q4
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q5
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q6
 priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q7
priority level 1
bandwidth percent 1
     output     : 1445 packets, 92536 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes
```



```
Class-map (queuing): mc-q2
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes
```

show queuing interface

Use this command to dispay the configurations of queues attached to an interface.

Command Syntax

```
show queuing interface NAME
```

Parameters

NAME	Interface name.

Command Mode

Exec & config mode

Applicability

This command was introduced before OcNOS version 1.3.

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 before OcNOS version 1.3.

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 map cos 0 queue 0
qos map cos 1 queue 1
qos map cos 2 queue 2
qos map cos 3 queue 3
qos map cos 4 queue 4
qos map cos 5 queue 5
qos map cos 6 queue 6
qos map cos 7 queue 7
qos map dscp 0 queue 0
qos map dscp 1 queue 0
qos map dscp 2 queue 0
qos map dscp 3 queue 0
qos map dscp 4 queue 0
qos map dscp 5 queue 0
qos map dscp 6 queue 0
qos map dscp 7 queue 0
qos map dscp 8 queue 1
qos map dscp 9 queue 1
qos map dscp 10 queue 1
qos map dscp 11 queue 1
qos map dscp 12 queue 1
qos map dscp 13 queue 1
```

```
qos map dscp 14 queue 1
qos map dscp 15 queue 1
qos map dscp 16 queue 2
qos map dscp 17 queue 2
qos map dscp 18 queue 2
qos map dscp 19 queue 2
qos map dscp 20 queue 2
qos map dscp 21 queue 2
qos map dscp 22 queue 2
qos map dscp 23 queue 2
qos map dscp 24 queue 3
qos map dscp 25 queue 3
qos map dscp 26 queue 3
qos map dscp 27 queue 3
qos map dscp 28 queue 3
qos map dscp 29 queue 3
qos map dscp 30 queue 3
qos map dscp 31 queue 3
qos map dscp 32 queue 4
qos map dscp 33 queue 4
qos map dscp 34 queue 4
qos map dscp 35 queue 4
qos map dscp 36 queue 4
qos map dscp 37 queue 4
qos map dscp 38 queue 4
qos map dscp 39 queue 4
qos map dscp 40 queue 5
qos map dscp 41 queue 5
qos map dscp 42 queue 5
qos map dscp 43 queue 5
qos map dscp 44 queue 5
qos map dscp 45 queue 5
qos map dscp 46 queue 5
qos map dscp 47 queue 5
qos map dscp 48 queue 6
qos map dscp 49 queue 6
qos map dscp 50 queue 6
qos map dscp 51 queue 6
qos map dscp 52 queue 6
qos map dscp 53 queue 6
qos map dscp 54 queue 6
qos map dscp 55 queue 6
qos map dscp 56 queue 7
qos map dscp 57 queue 7
qos map dscp 58 queue 7
qos map dscp 59 queue 7
qos map dscp 60 queue 7
qos map dscp 61 queue 7
qos map dscp 62 queue 7
qos map dscp 63 queue 7
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
```



```
  exit
class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit
!
interface xe1/1
 service-policy type queuing default default-out-policy
!
interface xe1/2
 service-policy type queuing default default-out-policy
!
interface xe1/3
 service-policy type queuing default default-out-policy
!
interface xe1/4
 service-policy type queuing default default-out-policy
!
interface xe2/1
 service-policy type queuing default default-out-policy
```

show running-config cpu-queue

Use this command to display details about CPU queue information based on processes running.

Command Syntax

```
show running-config cpu-queue
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#show running-config | in cpu-queue
cpu-queue sflow rate 10000 no-monitor
cpu-queue ospf rate 0 lossy monitor
cpu-queue nd rate 200 lossless monitor
cpu-queue arp rate 100 lossy no-monitor
cpu-queue bpdu rate 1000 monitor
```

trust dscp

Use this command to use dscp value to decide queue mapping for packets in Layer 2 interfaces.

The no parameter with this command un-sets trust dscp.

Command Syntax

```
trust dscp
```

```
no trust dscp
```

Parameters

None

Default

By default, trust dscp is enabled on L2 interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
#configure terminal
(config)#int xe1/1
(config-if)#trust dscp
```

wrr-queue weight

Use this command to set wrr-queue weight for a queue.

Use the priority level command to un-set configured wrr configuration.

Command Syntax

```
wrr-queue weight <1-127>
```

Parameters

<1-127>	wrr queue weight to be configured.

Default

No default value is specified

Command Mode

Policy-class-map queuing Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#policy-map type queuing default default-out-policy
(config-pmap-que-def)# class type queuing default q0
(config-pmap-c-que-def)#wrr-queue weight
(config-pmap-c-que-def)#wrr-queue weight 2
(config-pmap-c-que-def)#priority level 1
```

SECTION 8

Guest Virtual Machine

Guest Virtual Machine Command Reference

Contents

This document contains these chapters:

CHAPTER 1 Guest Virtual Machine Command Reference

This chapter contains the guest virtual machine commands.

debug vm-events

Use this command to log virtual machine operations.

Use the `no` form of this command to stop logging virtual machine operations.

Command Syntax

```
debug vm-events
no debug vm-events
```

Parameters

None

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug vm-events
```

dhcp-lease-max

Use this command to set the maximum number of DHCP leases for the VM bridge.

Command Syntax

```
dhcp-lease-max <10-1000>
```

Parameters

<10-1000>	Maximum number of DHCP leases

Default

The default maximum number of DHCP leases is 1000.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-lease-max 100
```

dhcp-lease-time

Use this command to set the maximum time for leasing an IP address for the VM bridge.

Command Syntax

```
dhcp-lease-time <2-3600>
```

Parameters

<2-3600>	Maximum time for leasing an IP address in minutes

Default

The default maximum time for leasing an IP address is 360 minutes.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-lease-time 1400
```

dhcp-range

Use this command to set a DHCP range for the virtual machine bridge.

Use the `no` form of this command to remove the DHCP range.

Command Syntax

```
dhcp-range A.B.C.D A.B.C.D
no dhcp-range
```

Parameters

`A.B.C.D`	Starting and ending IP address of the DHCP range

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-range 10.12.65.2 10.12.65.12
```

disk-image

Use this command to configure the disk image location for the VM template.

Command Syntax

```
disk-image DISK-IMAGE-LOCATION
```

Parameters

`DISK-IMAGE-LOCATION`

Location of the disk image to boot up the VM.

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#disk-image \sample_location
```

feature guest-vm

Use this command to enable the guest VM feature.

Use the `no` form of this command to disable the guest VM feature.

Command Syntax

```
feature guest-vm enable
no feature guest-vm enable
```

Parameters

None

Default

NA

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature guest-vm enable
```

gateway-ip

Use this command to set the gateway IP address for a virtual machine bridge.

Use the `no` form of this command to remove a gateway IP address.

Command Syntax

```
gateway-ip (A.B.C.D A.B.C.D | A.B.C.D/M)
no gateway-ip
```

Parameters

`A.B.C.D A.B.C.D`	Gateway IP address and subnet mask
`A.B.C.D/M`	Gateway IP address and subnet mask

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#gateway-ip 10.12.65.1/24
```

host-core-affinity

Use this command to set the core affinity value for a virtual machine template.

Use the `no` form of this command to set the core affinity value to its default.

Command Syntax

```
host-core-affinity AFFINITY-VALUE
no host-core-affinity
```

Parameters

`AFFINITY-VALUE` The core affinity values between 0 and 7.

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#host-core-affinity 6
```

iptables

Use this command to create a rule for the IP tables.

Use the `no` form of this command to remove an IP tables rule.

Command Syntax

```
iptables STRING (position POS_NUM |)
no iptables STRING
```

Parameters

`STRING`	Rule string in double quotes.
`POS_NUM`	Position to insert the rule string <1-65535>.

Default

NA.

Command Mode

IP tables mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables-template sample_template
(config-iptables)#iptables "INPUT DROP" position 65535
```

iptables restore

Use this command to restore the entries in the IP tables template to the IP tables.

Use the `no` form of this command to remove the entries in the IP tables.

Command Syntax

```
iptables restore iptables-template TEMPLATE_NAME (vrf VRF-NAME |)
no iptables restore (iptables-template TEMPLATE_NAME |) (vrf VRF-NAME |)
```

Parameters

`TEMPLATE-NAME`	Name of the IP tables template
`VRF-NAME`	Name of the VRF

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables restore iptables-template sample_template vrf VRF1
```

iptables-template

Use this command to create an IP tables template and enter IP tables mode.

Use the `no` form of this command to remove an IP tables template.

Command Syntax

```
iptables-template TEMPLATE_NAME
no iptables-template TEMPLATE_NAME
```

Parameters

`TEMPLATE_NAME`	Name of the IP tables template.

Default

NA.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables-template sample_template
(config-iptables)
```

memory

Use this command to configure the RAM size for the VM template.

Command Syntax

```
memory <128-8192>
```

Parameters

<128-8192>	Memory for Virtual Machine in MB

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#memory 1024
```

nat dnat

Use this command to set destination NAT addresses in the IP tables.

Use the `no` form of this command to remove the destination NAT addresses.

Command Syntax

```
nat dnat match-ip A.B.C.D to A.B.C.D (protocol (tcp | udp)|) (sport-num <0-65535>
  |) (dport-num <0-65535> |) (vrf VRF-NAME|)
no nat dnat match-ip A.B.C.D to A.B.C.D (protocol (tcp | udp)|) (sport-num <0-
  65535> |) (dport-num <0-65535> |) (vrf VRF-NAME|)
```

Parameters

`A.B.C.D`	From IP address
`A.B.C.D`	To IP address
`tcp`	Use TCP for NAT
`udp`	Use UDP for NAT
`sport-num`	Source port
`<0-65535>`	Source port number
`dport-num`	Destination port
`<0-65535>`	Destination port number
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nat dnat match-ip 1.1.1.1 to 1.1.1.2 protocol tcp
```

nat snat

Use this command to set the source NAT addresses in the IP tables.

Use the `no` form of this command to remove the source NAT addresses.

Command Syntax

```
nat snat from A.B.C.D/M to A.B.C.D (vrf VRF-NAME|)
no nat snat from A.B.C.D/M to A.B.C.D (vrf VRF-NAME|)
```

Parameters

`A.B.C.D/M`	From IP address and subnet mask
`A.B.C.D`	To IP address
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nat snat from 10.12.65.1 to 10.12.65.102 vrf VRF1
```

os-type

Use this command to configure the Operating System type of Virtual Machine.

Command Syntax

```
os-type (xen|linux|hvm|exe|uml)
```

Parameters

`xen`	Xen
`linux`	Linux
`hvm`	HVM
`exe`	Exe
`uml`	UML

Default

NA

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#os-type linux
```

os-variant

Use this command to set the operating system variant for a virtual machine template.

Use the `no` form of this command to remove the operating system variant.

Command Syntax

```
os-variant (generic|fedora|rhel|ubuntu|debian)
no os-variant (generic|fedora|rhel|ubuntu|debian)
```

Parameters

`generic`	Generic
`fedora`	Fedora
`rhel`	Red Hat Linux
`ubuntu`	Ubuntu
`debian`	Debian

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#os-variant debian
```

reload vm-name

Use this command to reload a running VM with a new template configuration.

Command Syntax

```
reload vm-name VM_NAME vm-template TEMPLATE_NAME
```

Parameters

VM-NAME	Name of the VM.
TEMPLATE-NAME	Name of the VM template.

Default

NA.

Command Mode

Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

#reload vm-name new vm-template sample

secondary-disk-image

Use this command to configure the secondary disk image location for the VM template.

Command Syntax

```
secondary-disk-image SECONDARY-DISK-IMAGE-LOCATION
no secondary-disk-image
```

Parameters

SECONDARY-DISK-IMAGE-LOCATION

Location of the secondary disk image to boot up the VM.

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#secondary-disk-image \sample_location
```

service dns-masq

Use this command to start the DHCP service in the virtual machne.

Use the `no` form of this command to stop the DHCP service.

Command Syntax

```
service dns-masq
no service dns-masq
```

Parameters

None

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#service dns-masq
```

show vm

Use this command to display the status of the virtual machine.

Command Syntax

```
show vm (details |) (VM_NAME |)
```

Parameters

`details`	Details
`VM_NAME`	Name of the virtual machine

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm
```

show vm-bridge

Use this command to display the bridge configuration.

Command Syntax

```
show vm-bridge (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-bridge
```

show vm-iptables

Use this command to display the IP tables.

Command Syntax

```
show vm-iptables (TEMPLATE_NAME | restored-iptables |)
```

Parameters

`TEMPLATE_NAME` Name of the IP tables template

`restored-iptables`
Restored IP tables

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-iptables
```

show vm-iptables kernel

Use this command to display the kernel IP tables.

Command Syntax

```
show vm-iptables kernel (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-iptables kernel
```

show vm-nat details

Use this command to display virtual machine NAT details.

Command Syntax

```
show vm-nat details (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-nat details
```

show vm-template

Use this command to display the status of the virtual machine template.

Command Syntax

```
show vm-template (VM-TEMP-NAME |)
```

Parameters

VM-TEMP-NAME	Name of the virtual machine template

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-template
```

start vm-name

Use this command to create a virtual machine (VM) based on the template configuration.

Use the `no` form of this command to end a running VM.

Command Syntax

```
start vm-name VM_NAME vm-template TEMPLATE_NAME
no start vm-name VM_NAME
```

Parameters

`VM-NAME`	Name of the VM
`TEMPLATE-NAME`	Name of the VM template

Default

NA

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# start vm-name new vm-template sample
(config)# exit

#configure terminal
(config)# no start vm-name new
(config)# exit
```

static-bind

Use this command to bind an IP address to a MAC address for the virtual machine.

Use the `no` form of this command to unbind an IP address from a MAC address.

Command Syntax

```
static-bind vm-mac-address XXXX.XXXX.XXXX ip-address A.B.C.D
no static-bind vm-mac-address XXXX.XXXX.XXXX ip-address A.B.C.D
```

Parameters

`XXXX.XXXX.XXXX`	MAC Address
`A.B.C.D`	IP Address

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#static-bind vm-mac-address ABCD.HHHH.EFGH.HHHH ip-address
10.12.65.102
```

stop vm-name

Use this command to stop arunning VM.

Command Syntax

```
stop vm-name VM_NAME
```

Parameters

VM-NAME	Name of the VM.

Default

NA

Command Mode

Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#stop vm-name new
```

vcpu count

Use this command to configure the virtual CPU count for the VM template.

Command Syntax

```
vcpu count <1-16>
```

Parameters

<1-16>	Virtual CPU count

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#vcpu count 16
```

virt-type

Use this command to set the virt-type as KVM or QEMU.

Command Syntax

```
virt-type (KVM | QEMU)
```

Parameters

KVM	Give VM
VQEMU	Give QEMU

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#virt-type kvm
(config-vm-temp)#virt-type qemu
```

virtual-nic

Use this command to set the MAC address of a virtual machine template.

Use the `no` form of this command to remove the MAC address.

Command Syntax

```
virtual-nic (vm-mac-addr XXXX.XXXX.XXXX|)(vrf VRF-NAME|)
no virtual-nic (vrf VRF-NAME|)
```

Parameters

`XXXX.XXXX.XXXX`	MAC address of the VM
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#virtual-nic vm-mac-address ABCD.HHHH.EFGH.HHHH vrf VRF1
```

vm-bridge-create

Use this command to create a virtual machine bridge and enter virtual machine bridge mode.

Use the `no` form of this command to remove a virtual machine bridge.

Command Syntax

```
vm-bridge-create VM-BRIDGE-NAME
no vm-bridge-create VM-BRIDGE-NAME
```

Parameters

`VM-BRIDGE-NAME` Name of the VM bridge.

Default

NA.

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)
```

vm-image delete

Use this command to delete a virtual machine image.

Command Syntax

```
vm-image delete VM_IMAGE_LOCATION
```

Parameters

VM_IMAGE_LOCATION

Location of the virtual machine image.

Default

NA.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-image delete \sample_location
```

vm-template

Use this command to create a virtual machine template and enter VM template mode.

Use the `no` form of this command to remove a virtual machine template.

Command Syntax

```
vm-template TEMPLATE_NAME
no vm-template TEMPLATE_NAME
```

Parameters

`TEMPLATE_NAME` Name of the VM template.

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#
```

SECTION 9

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.

802.1X. IEEE specification for port authentication.

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 4-189 compares the IPv4 and IPv6 address formats.

Table 4-189: 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 (.)
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.

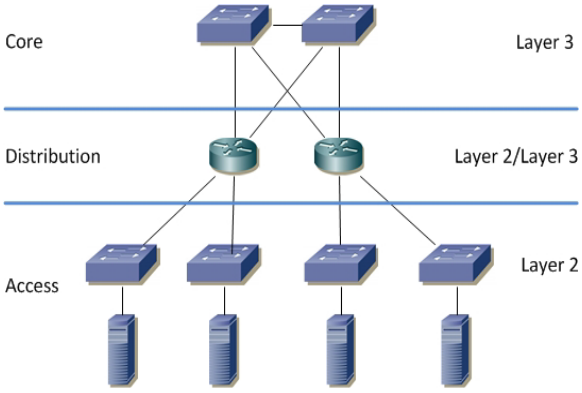
network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

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.

port authentication. A mechanism for port-based user authentication and network access control for LAN devices. Defined by IEEE 802.1X.

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 4-190 summarizes the characteristics of the dynamic routing protocols supported by OcNOS:

Table 4-190: 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 4-190: 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

TRansparent Interconnection of Lots of Links (TRILL). Layer 2 (L2) bridging using Intermediate System to Intermediate System (IS-IS) link-state routing. TRILL encapsulates native frames in a transport header that contains a hop count, routes the encapsulated frames using IS-IS, and decapsulates the native frame before delivery.

Spanning tree protocols restrict all traffic to a loop-free tree and in doing so creates blocking conditions that require the over provisioning of links. With TRILL, you can create a fully meshed network where all links are available on all paths, eliminating the need to over-provision links and improving the utilization of data center networking equipment.

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 10 Master Command Index

Master Command Index

SECTION 11 # 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