ipinfusion™

OcNOS®

Open Compute Network Operating System for Service Providers

Multicast Guide
Version 7.0.2
September 2026

IP Infusion Inc. Proprietary

© 2026 IP Infusion Inc. All Rights Reserved.

This documentation is subject to change without notice. The software described in this document and this documentation are furnished under a license agreement or nondisclosure agreement. The software and documentation may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of IP Infusion Inc.

IP Infusion Inc.

3979 Freedom Circle

Suite 900

Santa Clara, California 95054

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Trademarks:

IP Infusion and OcNOS are trademarks or registered trademarks of IP Infusion. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Use of certain software included in this equipment is subject to the IP Infusion, Inc. End User License Agreement at http://www.ipinfusion.com/license. By using the equipment, you accept the terms of the End User License Agreement.

Contents

Preface 11
Audience 11
Conventions 11
IP Infusion Product Release Version 11
Related Documentation 12
Feature Availability 12
Migration Guide 12
IP Maestro Support 12
Technical Support 12
. 14
Command Line Interface 15
Overview 15
Chapter Organization 15
Command Line Interface Help 15
Command Completion 16
Command Abbreviations 16
Command Line Errors 17
Command Negation 17
Syntax Conventions 17
Variable Placeholders 18
Command Description Format 19
Keyboard Operations 19
Show Command Modifiers 20
String Parameters 23
Command Modes 23
Transaction-based Command-line Interface 25
. 26

IGMP Configuration 27

CHAPTER 1 IGMP Configuration 28
IGMP Versions 28
IGMP Operation 28
Topology 29
IGMP Configuration 30

CHAPTER 2 IGMP Proxy Configuration 37
Terminology 37
Enabling IP Multicast Routing 39
Enabling Proxy upstream interface 39
Enabling Proxy downstream interface 39
Enabling Unsolicited report interval 41

CHAPTER 3 IGMP Snooping Configuration 43
Configuration 43

© 2026 IP Infusion Inc. Proprietary

IGMP Command Reference. 46

CHAPTER 1 Layer 3 IGMP Multicast Commands 47
clear ip igmp 48
debug ip igmp 49
ip igmp 51
ip igmp access-group 52
ip igmp immediate-leave 53
ip igmp join-group 54
ip igmp last-member-query-count 55
ip igmp last-member-query-interval 56
ip igmp limit 57
ip igmp mroute-proxy 58
ip igmp offlink 59
ip igmp proxy-service 60
ip igmp proxy unsolicited-report-interval 61
ip igmp querier-timeout 62
ip igmp query-interval 63
ip igmp query-max-response-time 64
ip igmp ra-option 65
ip igmp robustness-variable 66
ip igmp ssm-map enable 67
ip igmp ssm-map static 68
ip igmp static-group 69
ip igmp startup-query-count 70
ip igmp startup-query-interval 71
ip igmp version 72
show debugging ip igmp 73
show ip igmp groups 74
show ip igmp interface 76
show ip igmp proxy 78
show ip igmp ssm-map 80
show running-config interface igmp 81

CHAPTER 2 Layer 2 IGMP Snooping Multicast Commands 82
clear igmp snooping 83
igmp snooping 84
igmp snooping fast-leave 85
igmp snooping mrouter 86
igmp snooping querier 87
igmp snooping report-suppression 88
igmp snooping static-group 89
show igmp snooping interface 90
show igmp snooping groups 92
show igmp snooping mrouter 95
show igmp snooping statistics 96

Protocol Independent Multicasting Configuration 97

© 2026 IP Infusion Inc. Proprietary

CHAPTER 1 PIM Sparse Mode Configuration 98
Terminology 98
Data Flow from Source to Receivers in PIM-SM Network Domain 99
PIM-SM Configuration 100
IPV6 PIM-SM Configuration 101
Enabling IP Multicast Routing 102
Enable PIM-SM on an Interface 103
Enable PIM-SM Sub-Interface 103
Configuring Rendezvous Point Statically 104
Configure Rendezvous Point Dynamically Using Bootstrap Router Method 109
GROUP T0 RP MAPPING CONFIGURATION 117
Configure Static RP 117
Anycast-RP Configuration 119

CHAPTER 2 PIM Dense Mode Configuration 123
Terminology 123
Configuration 123
Enable PIM-DM Sub-Interface 128

CHAPTER 3 PIM-ECMP Redirect Configuration 130
Terminology 130
PIM-ECMP Configuration 131
Topology 131
Configure PIM ECMP Bundle 132
Bind PIM ECMP Bundle 132
Configure PIM ECMP 136
PIM-IPv6-ECMP Redirect Configuration 141

CHAPTER 4 PIM-BFD Configuration 146
PIM-BFD Configuration 146

CHAPTER 5 PIM Source-Specific Multicast Configuration 156
Overview 156
Feature Characteristics 156
PIM-SSM Configuration 156
Topology 157
Configuration 157

CHAPTER 6 . . . . . Bidirectional-PIM Configuration 163
Designated Forwarders (DF) Election 163
PIM-SM Configuration 163

CHAPTER 7 MSDP Configuration 169
Overview 169
Caching SA state 169
MSDP Mesh Group 169
MSDP Default Peer 170
Configure PIM-SM 170
Configure MSDP 170

© 2026 IP Infusion Inc. Proprietary

CHAPTER 8 VRRP Aware PIM Configuration 175
Topology 175

Protocol Independent Multicasting Command Reference 185

CHAPTER 1 PIMv4 Commands 186
clear ip mroute 188
clear ip msdp peer 190
clear ip msdp sa-cache 191
clear ip pim sparse-mode 192
debug ip pim 193
debug ip pim packet 194
debug pim bfd 195
debug ip pim timer assert 196
debug ip pim timer bsr 197
debug ip pim timer hello 198
debug ip pim timer joinprune 200
debug ip pim timer register 202
ip msdp default-peer 203
ip msdp mesh-group 204
ip msdp originator-id 205
ip msdp password 206
ip msdp peer 207
ip msdp sa 208
ip pim 209
p pim accept-register 210
ip pim anycast-rp 211
ip pim bfd 212
ip pim bfd all-interfaces 213
ip pim bidir-enable 214
ip pim bidir-offer-interval 215
ip pim bidir-offer-limit 216
ip pim bidir-neighbor-filter 217
ip pim bind ecmp-bundle 218
ip pim bsr-border 219
ip pim bsr-candidate 220
ip pim crp-cisco-prefix 221
ip pim dr-priority 222
ip pim ecmp-bundle 223
ip pim exclude-genid 224
ip pim hello-holdtime 225
ip pim hello-interval 226
ip pim ignore-rp-set-priority 227
ip pim jp-timer 228
ip pim neighbor-filter 229
ip pim passive 230
ip pim propagation-delay 231

© 2026 IP Infusion Inc. Proprietary

ip pim redundancy 232
ip pim register-rate-limit 233
ip pim register-rp-reachability 234
ip pim register-source 235
ip pim register-suppression 236
ip pim router-id 237
ip pim rp-address 238
ip pim rp-candidate 240
ip pim rp-register-kat 241
ip pim spt-threshold 242
ip pim ssm 243
ip pim state-refresh origination-interval 244
ip pim unicast-bsm 245
show debugging ip pim 246
show debugging pim 247
show ip msdp peer 248
show ip msdp sa-cache 249
show ip pim ecmp-bundle 251
show ip pim interface 252
show ip pim interface df 254
show ip pim mroute 255
show ip pim neighbor 257
show ip pim nexthop 260
show ip pim bsr-router 261
show ip pim local-members 263
show ip pim rp-hash 264
show ip pim rp mapping 265
snmp restart pim 266

CHAPTER 2 PIMv6 Commands 267
clear ipv6 mroute 269
clear ipv6 pim sparse-mode bsr 271
debug ipv6 pim 272
debug ipv6 pim packet 273
debug ipv6 pim timer assert 274
debug ipv6 pim timer bsr 275
debug ipv6 pim timer hello 276
debug ipv6 pim timer joinprune 277
debug ipv6 pim timer register 279
ipv6 pim 280
ipv6 pim accept-register 281
ipv6 pim anycast-rp 282
ipv6 pim bfd 283
ipv6 pim bfd all-interfaces 284
ipv6 pim bind ecmp-bundle 285
ipv6 pim bsr-border 286
ipv6 pim bsr-candidate 287

© 2026 IP Infusion Inc. Proprietary

ipv6 pim cisco-register-checksum 288
ipv6 pim crp-cisco-prefix 289
ipv6 pim dr-priority 290
ipv6 pim ecmp-bundle 291
ipv6 pim exclude-genid 292
ipv6 pim hello-holdtime 293
ipv6 pim hello-interval 294
ipv6 pim ignore-rp-set-priority 295
ipv6 pim jp-timer 296
ipv6 pim neighbor-filter 297
ipv6 pim passive 298
ipv6 pim propagation-delay 299
ipv6 pim register-rate-limit 300
ipv6 pim register-rp-reachability 301
ipv6 pim register-source 302
ipv6 pim register-suppression 303
ipv6 pim router-id 304
ipv6 pim rp-address 305
ipv6 pim rp-candidate 307
ipv6 pim rp embedded 308
ipv6 pim rp-register-kat 309
ipv6 pim spt-threshold 310
ipv6 pim ssm 311
ipv6 pim state-refresh origination-interval 312
ipv6 pim unicast-bsm 313
show debugging ipv6 pim 314
show ipv6 pim bsr-router 315
show ipv6 pim ecmp-bundle 317
show ipv6 pim interface 318
show ipv6 pim mroute 320
show ipv6 pim neighbor 323
show ipv6 pim nexthop 325
show ipv6 pim local-members 326
show ipv6 pim rp-hash 327
show ipv6 pim rp mapping 328

Multicast Listener Discovery Configuration 329

CHAPTER 1 MLD Configuration 330
Overview 330
Feature Characteristics 330
MLD Versions 330
MLD Leave Operation 331
Configuration 332
Topology 332
Configuration 332
Validation For MLDV2 336

Glossary 337

CHAPTER 2 MLD Proxy Configuration 338
Terminology 338
Enabling IPv6 Multicast Routing 340
Enabling Proxy upstream interface 340
Enabling Proxy downstream interface 340
Enabling Unsolicited report interval 342

CHAPTER 3 MLD Snooping Configuration 345
Overview 345
Feature Characteristics 345
MLD Snooping Configuration 346
Glossary 348

Multicast Listener Discovery Command Reference 350

CHAPTER 1 Layer 2 MLD Snooping Commands 351
clear mld snooping 352
mld snooping 353
mld snooping fast-leave 354
mld snooping mrouter 355
mld snooping querier 356
mld snooping report-suppression 357
show debugging mld snooping 358
show mld snooping mrouter 359
show mld snooping statistics 360
show mld snooping groups 361
show mld snooping interface 362

Multicast Command Reference 363

CHAPTER 1 Multicast Commands 364
clear ip mroute 365
debug ip mrib 366
ip mroute 367
ip multicast route-limit 368
ip multicast ttl-threshold 369
ip multicast-routing 370
ip multicast bidirectional enable 371
l2 unknown mcast 372
ipv6 mroute 373
show debugging ip mrib 374
show ip mroute 375
show ip mvif 378
show ip multicast rpa 380
show running-config interface multicast 381
snmp restart mribd 382

© 2026 IP Infusion Inc. Proprietary

CHAPTER 2 IPv6 Multicast Commands 383
clear ipv6 mroute 384
debug ipv6 mrib 385
ipv6 mroute 386
ipv6 multicast route-limit 387
ipv6 multicast-routing 388
ipv6 mroute 389
show debugging ipv6 mrib 390
show ipv6 mroute 391
show ipv6 mif 392
show running-config interface ipv6 multicast 393
snmp restart mrib 394

CHAPTER 3 Layer 3 MLD Multicast Commands 395
clear ipv6 mld 396
debug ipv6 mld 397
ipv6 mld 399
ipv6 mld access-group 400
ipv6 mld immediate-leave 401
ipv6 mld last-member-query-count 402
ipv6 mld last-member-query-interval 403
ipv6 mld limit 404
ipv6 mld mroute-proxy 405
ipv6 mld proxy unsolicited-report-interval 406
ipv6 mld proxy-service 407
ipv6 mld querier-timeout 408
ipv6 mld query-interval 409
ipv6 mld query-max-response-time 410
ipv6 mld robustness-variable 411
ipv6 mld ssm-map enable 412
ipv6 mld ssm-map static 413
ipv6 mld startup-query-count 414
ipv6 mld startup-query-interval 415
ipv6 mld static-group 416
ipv6 mld version 417
show debugging ipv6 mld 418
show ipv6 mld groups 419
show ipv6 mld interface 421
show ipv6 mld proxy 423
show ipv6 mld ssm-map 425

Index 426

© 2026 IP Infusion Inc. Proprietary

Preface

This guide describes how to configure OcNOS.

Audience

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

Conventions

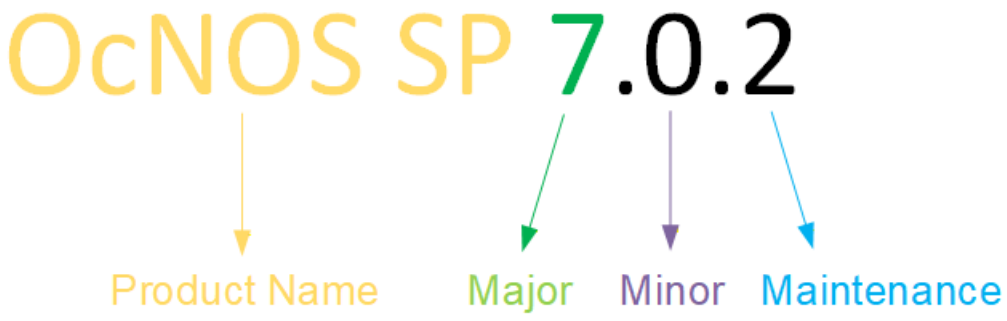
Table 1 on page 11 shows the conventions used in this guide.

Table 1: Conventions

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

IP Infusion Product Release Version

Each integer in release number indicates Major, Minor, and Maintenance release versions. Build numbers that follow the release numbers are for internal tracking and verification of the software build process and are visible to customers as part of the software version number.



Product Name: IP Infusion Product Family

Major Version: New customer-facing functionality that represents a significant change to the code base; including, a significant marketing change or direction in the product.

Minor Version: Enhancements or extensions to existing features, changes to address external needs, or internal ements might be motivated by improvements to satisfy new sales regions or marketing initiatives.

Maintenance Version: A collection of product bugs or hotfixes usually scheduled every 30 or 60 days, based on the number of hotfixes.

Related Documentation

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

Feature Availability

Each OcNOS SKU contains a set of supported features. For a list of available features based on the SKU that you purchased. Refer to the *Feature Matrix*.

Migration Guide

Check the *Migration Guide* for necessary configuration changes before migrating from one version of OcNOS to another.

IP Maestro Support

Monitor devices running OcNOS Release 6.3.4-70 and above using IP Maestro software.

Technical Support

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at the Technical Assistance Center.

Customers and partners enjoy full access to the support website. The site allows customers and partners to open technical support calls, update open calls with new information, and review the status of open or closed calls. The password-protected site includes technical documentation, Release Notes, and descriptions of service offerings.

Technical Sales

Contact the IP Infusion sales representative for more information about the OcNOS solution.

Technical Documentation

For core commands and configuration procedures, visit: Product Documentation.

For training videos, visit: OcNOS Free Training Videos.

For a list of supported platforms and SKUs of OcNOS features, refer to the OcNOS Feature Matrix.

Disclaimer

The global documentation site is evolving to provide an enhanced website user experience for select topics included in this release. Some guides are now available outside the existing documentation library and can be accessed directly from custom documentation landing pages. These guides offer robust in-built search functionality.

For the latest documentation, visit the product-specific documentation landing page and select the relevant guide.

Comments

If you have comments, or need to report a problem with the content, contact product-documentation@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.

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

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
```

© 2026 IP Infusion Inc. Proprietary

```
  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
```

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 int 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 2 on page 17 describes the conventions used to represent command syntax in this reference.

Table 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>)`

© 2026 IP Infusion Inc. Proprietary

Table 2: Syntax conventions (Continued)

Convention	Description	Example
`()`	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>}`
`[]`	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 3 on page 18 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table 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

© 2026 IP Infusion Inc. Proprietary

Table 3: Variable placeholders

Token	Description
`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 4 on page 19 explains the sections used to describe each command in this reference.

Table 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
Applicability	The command introduced in a specific release version and modified or updated in subsequent versions.
Example	An example of the command being executed

Keyboard Operations

Table 5 on page 19 lists the operations you can perform from the keyboard.

Table 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.

© 2026 IP Infusion Inc. Proprietary

Table 5: Keyboard operations (Continued)

Key combination	Operation
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
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[2-4]

...skipping
interface xe2
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 2
!
route-map mymap1 permit 10
!
route-map rmap1 permit 2
!
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
```

String Parameters

The restrictions in Table 6 on page 23 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table 6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “|”, and “=” The “|” character is allowed only for the `description` command in interface mode.

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-7 lists the command modes common to all protocols.

Table 7: 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`, 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. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

© 2026 IP Infusion Inc. Proprietary

Command Mode Tree

The diagram below shows the common command mode hierarchy.

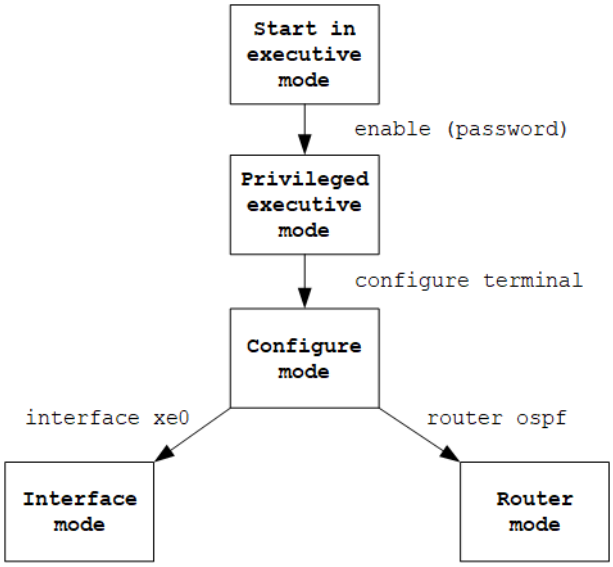


Figure 1: Common command modes

To change modes:

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

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

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

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

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the `show transaction current` command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the `commit` command.
- If a `commit` fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the `commit`.
- Discard the candidate configuration with the `abort transaction` command.
- Check the last aborted transaction with the `show transaction last-aborted` command.
- Multiple configurations cannot be removed with a single `commit`. You must remove each configuration followed by a `commit`.

Note: All commands MUST be executed only in the default CML shell (`cmlsh`). If you log in as root and start `imish`, then the system configurations will go out of sync. The `imish` shell is not supported and should not be started manually.

© 2026 IP Infusion Inc. Proprietary

IGMP Configuration

© 2026 IP Infusion Inc. Proprietary

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 1-1.

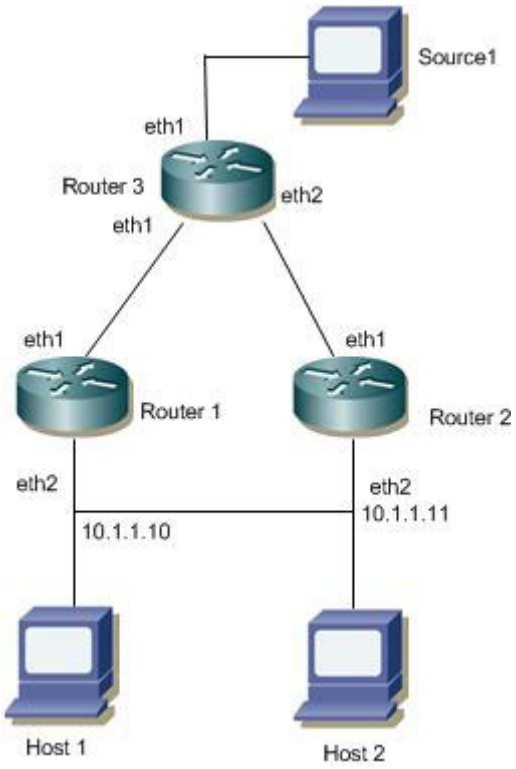


Figure 1-1: IGMP Topology

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)#commit`	Commit the transaction.
`(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)#commit`	Commit the transaction.
`(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
```

© 2026 IP Infusion Inc. Proprietary

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 1-1: IGMP group table after IGMPV2 membership report

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
Rtr1#show  ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime     Expires     State     Last Reporter
224.0.1.3            eth2       00:10:06   00:03:43    Active    10.1.1.52
224.1.1.1            eth2       01:54:53   static      Active    0.0.0.0
225.1.1.1            eth2       00:17:22   static      Active    0.0.0.0
```

```
Rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
State: Active
Last reporter:  10.1.1.52
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          225.1.1.1
```

```
Flags:          SG
Uptime:         00:17:28
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty
```

IGMP Group Table after IGMPV3 Membership report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface. Here IGMPV3 should be configured on the interface (by default IGMPv3 will be enabled if pim is configured on the interface).

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-2: 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.

© 2026 IP Infusion Inc. Proprietary

IGMP-Proxy Configuration Steps

This section provides the configuration steps for configuring IGMP Proxy and example for a relevant scenario.

- Enable IP multicast on each router (see Enabling IP Multicast Routing)
- Enable IGMP Proxy service on the upstream interface.
- Enable IGMP mroute configuration on the downstream interface.
- Enable IGMP proxy unsolicited report interval on the proxy interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time. This is an optional parameter in which the default value of 1 sec is considered for forwarding proxy groups to upstream router.

Note: Configure IP addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

In this network topology, Router 1 acts as a proxying router to the upstream router Router 2 in which PIM domain is present. Also the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

Note: Any PIM mode (PIM-SM,PIM-DM,PIM-SMDM) should be enabled on all the interfaces in the PIM domain.

Here in this example default value for unsolicited report interval is considered.

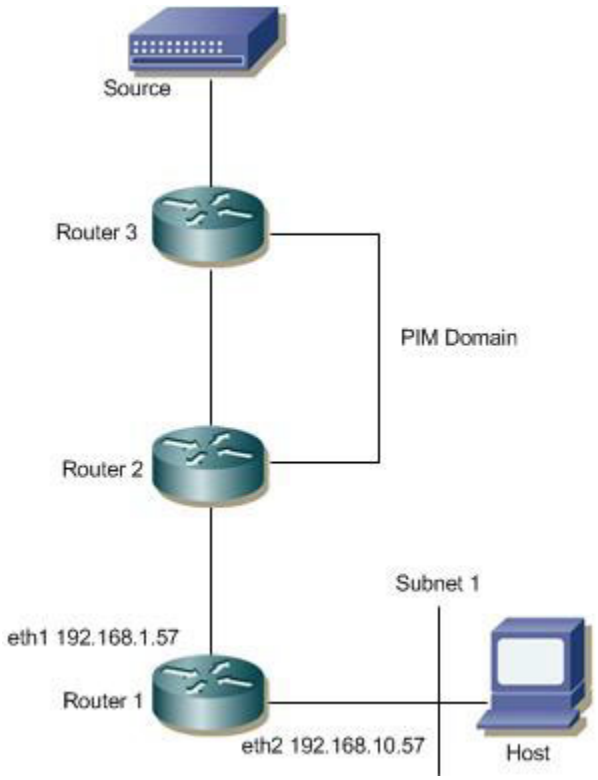


Figure 2-2: IGMP Proxy Topology

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)#commit`	Commit the transaction.

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)#commit`	Commit the transaction.
`(config)#exit`	Exit Configure mode.

Enabling Proxy downstream interface

Enable IGMP mroute proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Enter Interface mode
`(config-if)#ip address 192.168.10.57/24`	Assign IP address to an interface
`(config-if)#ip igmp mroute-proxy eth1`	Enable IGMP mroute proxy on the downstream interface and specify the upstream proxy interface name.
`(config-if)#commit`	Commit the transaction.
`(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)#commit`	Commit the transaction.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface eth0
!
```

```
interface eth1
ip address 192.168.1.57/24
ip igmp proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface eth2
ip address 192.168.10.57/24
ip igmp mroute-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

The following output displays the IGMP proxy unsolicited report interval information.

```
Router1#show ip igmp interface eth1

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 20000 milliseconds
```

IGMP proxy group with unsolicited report interval

The following output displays the IGMP proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Idle
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

CHAPTER 3 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.

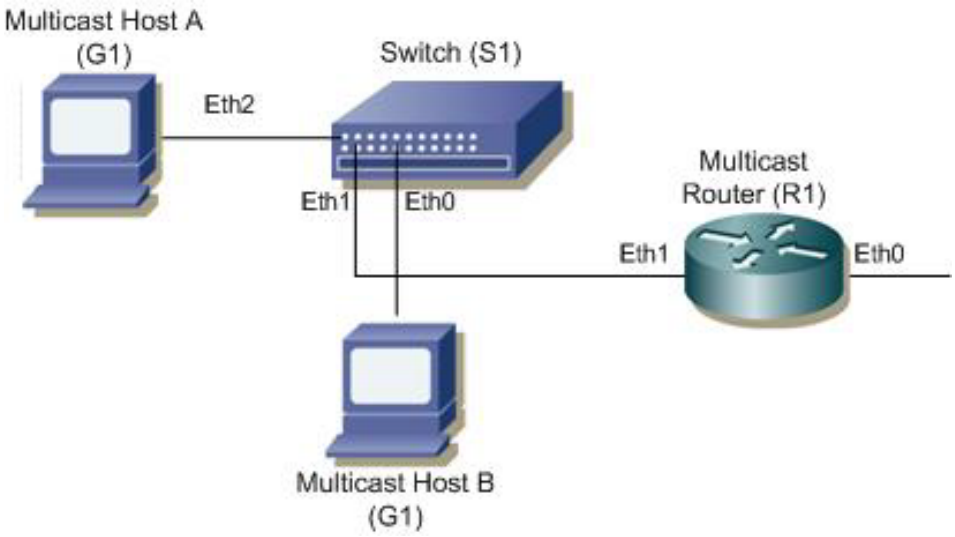


Figure 3-3: IGMP Snooping Topology

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

Note: Execute l2 unknown mcast CLI to enable the option to drop the unknown multicast traffic.

S1

`#configure terminal`	Enter the `Configure` mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Add bridge `1` to the spanning-tree table.
`(config)#interface eth0`	Specify the interface `eth0` to be configured, and enter the `Interface` mode.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth1`	Specify interface `eth1` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth2`	Specify interface `eth2` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth2` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface vlan1.1`	Specify interface `vlan1.1` to be configured.
`(config-if)# igmp snooping mrouter interface eth1`	Configure this port as a multicast router port
`(config-if)#commit`	Commit the transaction.

Validation

```
#show running-config interface eth0
!
interface eth0
switchport
bridge-group 1
switchport mode access
!
#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode access
!

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode access
!

#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan Group/Source Address Interface Flags Uptime Expires Last Reporter Version
1 224.1.1.1 eth0 R 00:00:03 00:04:17 0.0.0.0 V3
1 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0 V3

#show igmp snooping interface vlan1.1
IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 1
Number of Groups: 1
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 2
Active Ports:
eth0
eth1
eth2
```

IGMP Command Reference

© 2026 IP Infusion Inc. Proprietary

CHAPTER 1 Layer 3 IGMP Multicast Commands

This chapter describes the commands for Internet Group Management Protocol (IGMP) including the IGMP proxy service.

For IGMP multicast snooping commands, see Chapter 2, *Layer 2 IGMP Snooping Multicast Commands*.

- clear ip igmp
- debug ip igmp
- ip igmp
- ip igmp access-group
- ip igmp immediate-leave
- ip igmp join-group
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp limit
- ip igmp mroute-proxy
- ip igmp offlink
- ip igmp proxy-service
- ip igmp proxy unsolicited-report-interval
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp ra-option
- ip igmp robustness-variable
- ip igmp ssm-map enable
- ip igmp ssm-map static
- ip igmp static-group
- ip igmp startup-query-count
- ip igmp startup-query-interval
- ip igmp version
- show debugging ip igmp
- show ip igmp groups
- show ip igmp interface
- show ip igmp proxy
- show ip igmp ssm-map
- show running-config interface igmp

© 2026 IP Infusion Inc. Proprietary

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 xe1
(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)#interface xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(config-if)#ip igmp mroute-proxy xe1
```

ip igmp offlink

Use this command to enable IGMP offlink processing on an interface.

IGMP offlink allows the router to process IGMP reports or leaves that originate from non-local (non-native) subnets. This is typically required in scenarios where IGMP reports are forwarded by downstream routers or proxies that reside in a different subnet.

When the `log-suppress` parameter is configured, the system suppresses warning-level log messages generated for non-local IGMP reports or leaves. This reduces log volume in environments with many offlink receivers.

Use the `no` parameter with this command to disable IGMP offlink processing on an interface.

Note:

- Applicable only for IGMPv2 and IGMPv3 (IPv4 multicast).
- MLD (IPv6 multicast) is not supported.
- Disabling IGMP (`no ip igmp`) automatically removes any configured `ip igmp offlink` and `ip igmp offlink log-suppress` options.

Command Syntax

```
ip igmp offlink (log-suppress|)
no ip igmp offlink (log-suppress|)
```

Parameter

`log-suppress`	(Optional) Suppresses warning-level log messages for IGMP reports or leaves received from non-local subnets.

Command Mode

Interface mode

Default

Disabled

Applicability

Introduced before OcNOS version 1.3. Added a parameter `log-suppress` in OcNOS version 7.0.0.

Examples

The `ip igmp offlink` command allows the interface to process IGMP reports from non-local subnets.

```
#configure terminal
(config)#interface xe48
(config-if)#ip igmp offlink
(config-if)#no ip igmp offlink
```

The `log-suppress` parameter prevents warning messages from being generated for these non-local reports, reducing log volume in high-receiver scenarios.

```
(config-if)#ip igmp offlink log-suppress
(config-if)#no ip igmp offlink log-suppress
```

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 xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(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 xe1
(config-if)#ip igmp static-group 226.1.2.3

#configure terminal
(config)#interface xe1
(config-if)#ip igmp static-group 226.1.2.4 source 1.2.3.4

#configure terminal
(config)#interface xe1
(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 xe1
(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 xe1
(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 xe1
(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 1-3 shows the flags codes displayed at the start of a group entry.

Table 1-3: Flags

Flag	Meaning
M	Source Specific Multicast
R	Remote multicast
L	Local multicast
SG	Static Group
SS	Static Source

Table 1-4 explains the output fields.

Table 1-4: 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 1-3.
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 1-3.
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 1-3.

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 1-5 explains the output fields.

Table 1-5: 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 1-5: 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 1-6 explains the output fields.

Table 1-6: 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 1-7 explains the output fields.

Table 1-7: 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.

© 2026 IP Infusion Inc. Proprietary

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 2 Layer 2 IGMP Snooping Multicast Commands

This chapter describes commands for Internet Group Management Protocol (IGMP) multicast snooping.

- clear igmp snooping
- igmp snooping
- igmp snooping fast-leave
- igmp snooping mrouter
- igmp snooping querier
- igmp snooping report-suppression
- igmp snooping static-group
- show igmp snooping interface
- show igmp snooping groups
- show igmp snooping mrouter
- show igmp snooping statistics

© 2026 IP Infusion Inc. Proprietary

clear igmp snooping

Use this command to clear IGMP snooping groups and interface.

Command Syntax

```
clear igmp snooping group *
clear igmp snooping group A.B.C.D (IFNAME|)
clear igmp snooping interface IFNAME
```

Parameters

`*`	Displays all groups
`IFNAME`	The name of the VLAN interface
`A.B.C.D`	Multicast group Address

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#clear igmp snooping group *
```

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 (disable|enable)
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 enable
```

© 2026 IP Infusion Inc. Proprietary

igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the IGMP group-membership is removed as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the `no` parameter with this command to disable fast-leave processing.

Command Syntax

```
igmp snooping fast-leave
no igmp snooping fast-leave
```

Parameters

None

Default

IGMP Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable fast-leave processing on a VLAN.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping fast-leave
```

igmp snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the `no` parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax

```
igmp snooping mrouter interface IFNAME
no igmp snooping mrouter interface IFNAME
```

Parameter

`IFNAME`	Specify the name of the interface.

Default

IGMP Snooping mrouter processing is disabled.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows interface fe8 statically configured to be a multicast router interface.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping mrouter interface fe8
```

igmp snooping querier

Use this command to enable IGMP snooping querier functionality on a VLAN when IGMP is not enabled on the particular VLAN. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

The IGMP Snooping querier uses the 0.0.0.0 source IP address, because it only masquerades as a proxy IGMP querier for faster network convergence. It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router. It restarts as the IGMP Snooping querier if no queries are seen within the other querier interval.

Use the `no` parameter with this command to disable IGMP querier configuration.

Command Syntax

```
igmp snooping querier
no igmp snooping querier
```

Default

By default, Querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping querier
```

igmp snooping report-suppression

Use this command to enable report suppression for IGMP version 1, 2 and 3 reports.

Use the `no` parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping report-suppression (disable|enable)
no igmp snooping report-suppression
```

Default

By default, report suppression is enabled on x86.

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping report-suppression enable
```

igmp snooping static-group

Use this command to statically configure group membership entries on an interface

Use the `no` parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping static-group A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D interface IFNAME
igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
```

Parameters

`IFNAME`	Specify the name of the interface.
`A.B.C.D`	Specify the IP address In case of static-group, Multicast Address to be Joined. In case of source, Source Address to be Joined.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#conf t
(config)#interface vlan1.1
(config-if)#igmp snooping static-group 230.0.0.1 interface xe2
(config-if)#igmp snooping static-group 230.0.0.1 source 10.10.10.10 interface
xe1
(config-if)#exit
(config)#exit
```

show igmp snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax

```
show igmp snooping interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Default

By default, report suppression is disabled on Qumran devices.

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces.

```
#show igmp snooping interface
Global IGMP Snooping information
IGMP Snooping Enabled
IGMPv1/v2 Report suppression Enabled
IGMPv3 Report suppression Enabled
IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
xe5/1
IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds

IGMP Snooping information for vlan1.2
```

```
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds
IGMP Snooping maximum query response time is 10 seconds
IGMP Snooping Startup query interval is 31 seconds
Querier robustness: 2
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
xe5/1
```

show igmp snooping groups

Use this command to display the multicast groups learnt through snooping or statically configured.

Command Syntax

```
show igmp snooping groups
show igmp snooping groups details
show igmp snooping groups A.B.C.D
show igmp snooping groups A.B.C.D detail
show igmp snooping groups IFNAME
show igmp snooping groups IFNAME A.B.C.D
show igmp snooping groups IFNAME A.B.C.D detail
show igmp snooping groups IFNAME detail
```

Parameters

`A.B.C.D`	Specify multicast group address.
`IFNAME`	Specify the name of the interface.
`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
200   230.0.0.1             xe1          S     00:02:07   static   0.0.0.0
V3
#show igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      xe1
Group:          230.0.0.1
Flags:          S
Uptime:         00:02:08
Group mode:     Exclude (Static)
Last reporter:  0.0.0.0
Source list is empty

#show igmp snooping groups 230.0.0.1
```

```
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:35   static   0.0.0.0
V3
      #show igmp snooping groups 230.0.0.1 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:37
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty

      #show igmp snooping groups vlan1.200
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:47   static   0.0.0.0
V3
      #show igmp snooping groups vlan1.200 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:50
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty
```

Table 2-8: 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 2-8: 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 Configuration

© 2026 IP Infusion Inc. Proprietary

CHAPTER 1 PIM Sparse Mode

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.

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.

© 2026 IP Infusion Inc. Proprietary

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

Protocol Independent Multicast - Sparse Mode (PIM-SM) is a multicast routing protocol that uses an explicit join model to deliver data only to network segments that have active receivers. Unlike dense mode protocols that flood traffic, PIM-SM is designed for environments where group members are sparsely distributed across the network. It relies on a central point known as the Rendezvous Point (RP) to coordinate the delivery of multicast traffic from sources to receivers.

Feature Description

PIM-SM constructs a unidirectional shared tree (RPT) rooted at the RP to distribute traffic from sources to receivers. When a source begins sending data, its local first-hop router encapsulates the data in Register messages and sends

them to the RP. Receivers join the shared tree by sending Join messages toward the RP. PIM-SM also supports the transition to a Shortest Path Tree (SPT) for more efficient data delivery directly from the source to the receiver. The protocol operates independently of the underlying unicast routing protocol, though it relies on the unicast routing table for Reverse Path Forwarding (RPF) checks.

Benefits

- Efficient Bandwidth Usage: Traffic is only sent to branches of the network where receivers have explicitly requested it, reducing unnecessary overhead.
- Scalability: By utilizing a Rendezvous Point (RP), the protocol effectively manages multicast groups across large, complex provider networks.
- Resource Conservation: Minimizes the processing load on routers by avoiding the "flood and prune" behavior characteristic of dense mode protocols.
- Protocol Independence: Works seamlessly with various unicast routing protocols like OSPF to determine the best paths for multicast distribution.

Prerequisites

Before configuring PIM-SM, ensure the following foundational network settings are in place:

- Unicast Routing: A unicast routing protocol (such as OSPF) must be operational across the domain to provide reachability and facilitate RPF checks.
- IP Connectivity: All participating interfaces must have valid IP addresses (IPv4 or IPv6) and be in an 'up' state.
- IGMP/MLD: Internet Group Management Protocol (IGMP) for IPv4 or Multicast Listener Discovery (MLD) for IPv6 must be enabled on interfaces connected to receivers.

Topology

The topology consists of three primary OcNOS routers (Router-1, Router-2, and Router-3) forming a multicast domain.

- Router-2 serves as the Rendezvous Point (RP), configured with a Loopback interface (lo) address of 26.0.0.5 for IPv4 and 1201::8 for IPv6.
- Router-1 and Router-3 act as PIM Sparse Mode routers.
- The routers are interconnected via board interfaces (xe12, xe5, ce2, ce0).
- OSPF is used as the underlying IGP to provide unicast reachability between all routers and the RP.

© 2026 IP Infusion Inc. Proprietary

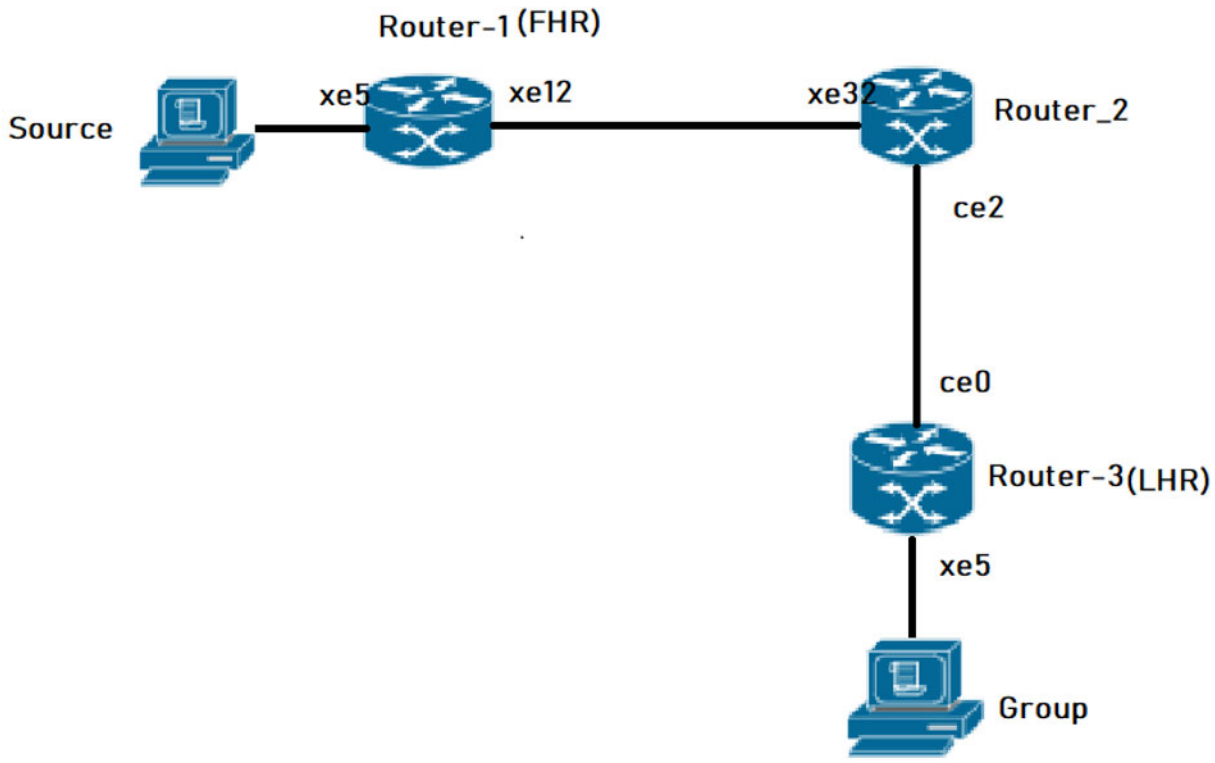


Figure 1-4: PIM-SM Topology

Configuration

The following PIM Sparse Mode configurations apply to all PIM routers within the OcNOS multicast domain:

1. Enable global multicast routing for both IPv4 and IPv6 to allow the router to process and forward multicast packets across its interfaces.

```
(config)# ip multicast-routing
(config)# ipv6 multicast-routing
(config)# commit
```

2. Enable PIM Sparse Mode on physical interfaces to allow the exchange of PIM neighbor discovery and join/prune messages, facilitating the construction of the multicast tree.

```
(config)# interface xe12
(config-if)# ip pim sparse-mode
(config-if)# ipv6 pim sparse-mode
(config-if)# commit
```

3. Configure a static Rendezvous Point (RP) address to provide a consistent meeting point for sources and receivers throughout the PIM domain.

```
(config)# ip pim rp-address 26.0.0.5
(config)# ipv6 pim rp-address 1201::8
(config)# commit
```

© 2026 IP Infusion Inc. Proprietary

Note: The configurations for Router-1 are shown as a sample; configurations for Router-2 and Router-3 are similar, ensuring interface-specific IP addresses and OSPF parameters are adjusted to match the topology.

Validation

To verify the PIM-SM configuration and operation, use the following show commands.

Verify PIM Interface Status. Check that PIM is active on the intended interfaces and verify the Designated Router (DR) election.

```
Router-1# show ip pim interface
Total number of PIM interfaces:2
Address          Interface   VIFindex   Ver/   Nbr    DR         DR
                                        Mode   Count  Prior
70.1.1.2         xe5         0          v2/S   0      1          70.1.1.2
20.1.1.2         xe12        2          v2/S   1      1          20.1.1.2

Router-1#show ipv6 pim interface
Total number of PIM interfaces:2
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Prior
xe5       2        v2/S   0      1
    Address       : fe80::5e07:58ff:fe28:b335
    Global Address: 7001::2
    DR            : this system
xe12      0        v2/S   1      1
    Address       : fe80::5e07:58ff:fe28:b33c
    Global Address: 2001::2
    DR            : fe80::5e07:58ff:fe6f:ff12
```

Verify PIM Neighbors

Ensure that PIM adjacency is established between neighboring routers to allow multicast control traffic flow.

```
router-2#show ip pim neighbor
Total number of PIM neighbors:2
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
30.1.1.2        ce2                00:37:56/00:01:19         v2    1 / DR
20.1.1.2        xe32               00:41:37/00:01:38         v2    1 / DR
router-2#show ipv6 pim neighbor
Total number of PIM neighbors:2
Neighbor Address                         Interface   Uptime/Expires    DR
                                                                       Pri/Mode
fe80::5e07:58ff:fe28:b30a                ce2         00:38:11/00:01:34 1 /
fe80::5e07:58ff:fe28:b33c                xe32        00:47:00/00:01:34 1 /
router-2#sho ipv6 ospf neighbor
Total number of full neighbors: 2
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
6.6.6.6           1   Full/Backup     00:00:29    ce2        0
8.8.8.8           1   Full/DR         00:00:39    xe32       0
```

Verify RP Mappings Confirm that the router correctly identifies the static RP for the multicast group ranges.

```
router-2#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 26.0.0.5
    Uptime: 00:48:23
```

Note: At Router-2, the `show ipv6 pim rp mapping` command shows that 1201::8 is the RP for all multicast groups ff00::8 and is statically configured. All other routers will have a similar output:

```
router-2#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Group(s): ff00::/8, Static
    RP: 1201::8
    Uptime: 00:50:17
```

Verify Multicast Routing Table

The mroute table shows the active multicast entries, including the incoming interface (IIF) and outgoing interface list (OIL).

Note: At Router-2, the `show ipv6 pim rp mapping` command shows that 26.0.0.5 is the RP for all multicast groups in the range 224.0.0.0/4, and it is statically configured. All other routers display similar output:

```
Router-3#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)
(70.1.1.3, 225.1.1.5), uptime 00:02:36, stat expires 00:02:10
Owner PIM, Flags: TF
  Incoming interface: ce0
  Outgoing interface list:xe5(1)
router-2#sho ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 26.0.0.5
    Uptime: 00:48:23

The show ipv6 pim mroute command displays the IPv6 multicast routing table. In this
table, the following fields are defined:
R-E#show ipv6 pim mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 5
(S,G) Entries: 5
(S,G,rpt) Entries: 5
FCR Entries: 0
```

```
(*, ff1e::1)
RP: 1001::1
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    ..j...........................
 Asserted  ..............................
FCR:
```

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.

Note: At Router-2, the show ipv6 pim rp mapping command shows that 1201::8 is the RP for all multicast groups ff00::8 and is statically configured. All other routers will have a similar output:

```
router-2#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Group(s): ff00::/8, Static
    RP: 1201::8
    Uptime: 00:50:17
```

Implementation Example

Use Case: Enterprise Video Distribution An organization needs to stream high-definition training videos to multiple offices without saturating the network.

Solution: Implementing PIM-SM allows the video source to send a single stream to the RP. Only routers with employees actively watching the stream will join the shared tree and receive the traffic, ensuring efficient bandwidth utilization across the provider backbone.

Configuring Rendezvous Point Statically

In a Protocol Independent Multicast Sparse Mode (PIM-SM) domain, each multicast group must map to a single Rendezvous Point (RP). The RP acts as the root of the group-specific shared distribution tree (RPT). All routers within the PIM domain must know the RP address to correctly forward multicast Join and Register messages.

When you configure the RP statically, you manually define the RP IP address on every router in the PIM domain. Each router must maintain an identical RP-to-group mapping to ensure end-to-end multicast reachability.

Feature Characteristics

- Each multicast group requires exactly one RP address within the PIM domain.
- All routers must map the group to the same RP address.
- Configure the RP address on every router, including routers that:
  - Do not have directly connected multicast sources.
  - Do not have directly connected multicast receivers.
- The network can support multiple RPs.
- Each RP can serve different multicast groups.
- A single multicast group must map to only one RP.
- Static configuration does not use Auto-RP or BSR mechanisms.
- Routers do not dynamically learn RP information.
- Static RP configuration does not provide redundancy.

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 1-4, `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`).

Benefits

- All routers use a fixed, administrator-defined RP address. The mapping does not change unless manually modified.
- Simple Deployment
- No dynamic RP advertisement or election mechanisms are required.
- The configuration eliminates RP discovery traffic.
- Suitable for Small and Stable Networks
- The approach is appropriate when:
  - The number of multicast groups is limited.
  - RP reassignment is infrequent.
  - The network size is small.

Configuration

For configurations refer PIM Sparse Mode Configuration.

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#
At Router_D, the show ipv6 pim rp mapping command shows that 1001::1 is the RP
for all multicast groups  ff00::8 and is statically configured. All other
routers will have a similar output:
R-D#show ipv6 pim rp-mapping
    PIM Group-to-RP Mappings
    Override RP cnt: 0


    Group(s): ff00::/8, Static
       RP: 1001::1
         Uptime: 01:21:47
    Embedded RP Groups
```

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 ipv6 pim rp-hash ff11::2
RP: 1222::2
```

Override RP cnt: 0At Router_D, use the show ipv6 pim rp-hash command to display the selected RP for a specified group (ff02::1).

```
Router_D#show ipv6 pim rp-hash
      RP: 1001::1
```

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
FOR IPV6
#show ipv6 pim neighbor

Total number of PIM neighbors:2

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::eac5:7aff:fea8:7cb9                 eth1        01:29:52/00:01:18  1 /
fe80::eac5:7aff:feb1:6b13                 eth2        01:29:49/00:01:28  1 /
```

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:
```

The `show ipv6 pim mroute` command displays the IPv6 multicast routing table. In this table, the following fields are defined:

```
R-E#show ipv6 pim mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 5
(S,G) Entries: 5
(S,G,rpt) Entries: 5
FCR Entries: 0

(*, ff1e::1)
RP: 1001::1
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     .............................
 Joined    ..j..........................
 Asserted  .............................
FCR:
```

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  ..............................
FOR IPV6
#show ipv6 pim mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 5
(S,G) Entries: 5
(S,G,rpt) Entries: 5
FCR Entries: 0

(*, ff1e::1)
RP: 1001::1
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    ..j............................
 Asserted  ..............................
FCR:
```

Implementations Example

Small Enterprise Multicast Deployment:

Scenario

An enterprise network deploys Protocol Independent Multicast Sparse Mode to support internal video distribution and software update streaming.

The multicast domain contains 8 routers and fewer than 10 multicast groups.

Design Decision:

- One router in the core acts as the RP.

- The administrator configures the same RP address on all routers.
- No redundancy is required.
- The topology remains stable.

Why Static RP is Appropriate:

- Limited number of routers.
- No requirement for RP failover.
- Low operational complexity.
- Predictable multicast forwarding behavior.

PIM Bootstrap Router

The Bootstrap Router (BSR) mechanism is a dynamic method for configuring Rendezvous Points (RP) within a Protocol Independent Multicast (PIM) Sparse Mode domain. It eliminates the need for manual, static RP assignments on every router, which is particularly critical for large or complex multicast networks. The BSR acts as a central distribution point, ensuring all routers in the domain learn the group-to-RP mappings necessary for multicast traffic forwarding.

Feature Description

In a PIM domain, the BSR mechanism utilizes a set of configured Candidate-BSRs (C-BSRs) and Candidate-RPs (C-RPs). Through an election process, the C-BSR with the highest priority value is elected as the BSR for the domain.

Once elected, the BSR performs the following technical functions:

- Candidacy Collection: C-RPs report their availability and the multicast groups they support to the elected BSR.
- RP Set Distribution: The BSR selects a subset of these C-RPs and distributes the group-to-RP mappings to all PIM routers via Bootstrap Messages (BSM).
- RP Election: When multiple RPs support the same group, routers select the RP with the lowest priority value. If priorities are equal, a hash function is applied to ensure a consistent RP choice across the domain.

Benefits

- Scalability: Automates RP distribution, making it ideal for large networking environments.
- Reduced Administrative Overhead: Eliminates repetitive manual configurations on every router when RPs change or fail.
- Fault Tolerance: If a primary RP fails, the BSR mechanism allows the network to dynamically switch to another Candidate-RP.
- Consistency: The hash mechanism ensures all routers in the PIM domain maintain an identical view of group-to-RP mappings.

Prerequisites

Before configuring BSR, ensure that the underlying Interior Gateway Protocol (IGP) such as OSPF or IS-IS is fully operational to provide reachability. Multicast routing must be enabled globally on all participating nodes.

- Essential Preliminary Configurations:
- Enable Multicast Routing: Both IPv4 and IPv6 multicast routing must be active.
- PIM Sparse Mode: PIM sparse-mode must be enabled on all participating interfaces.

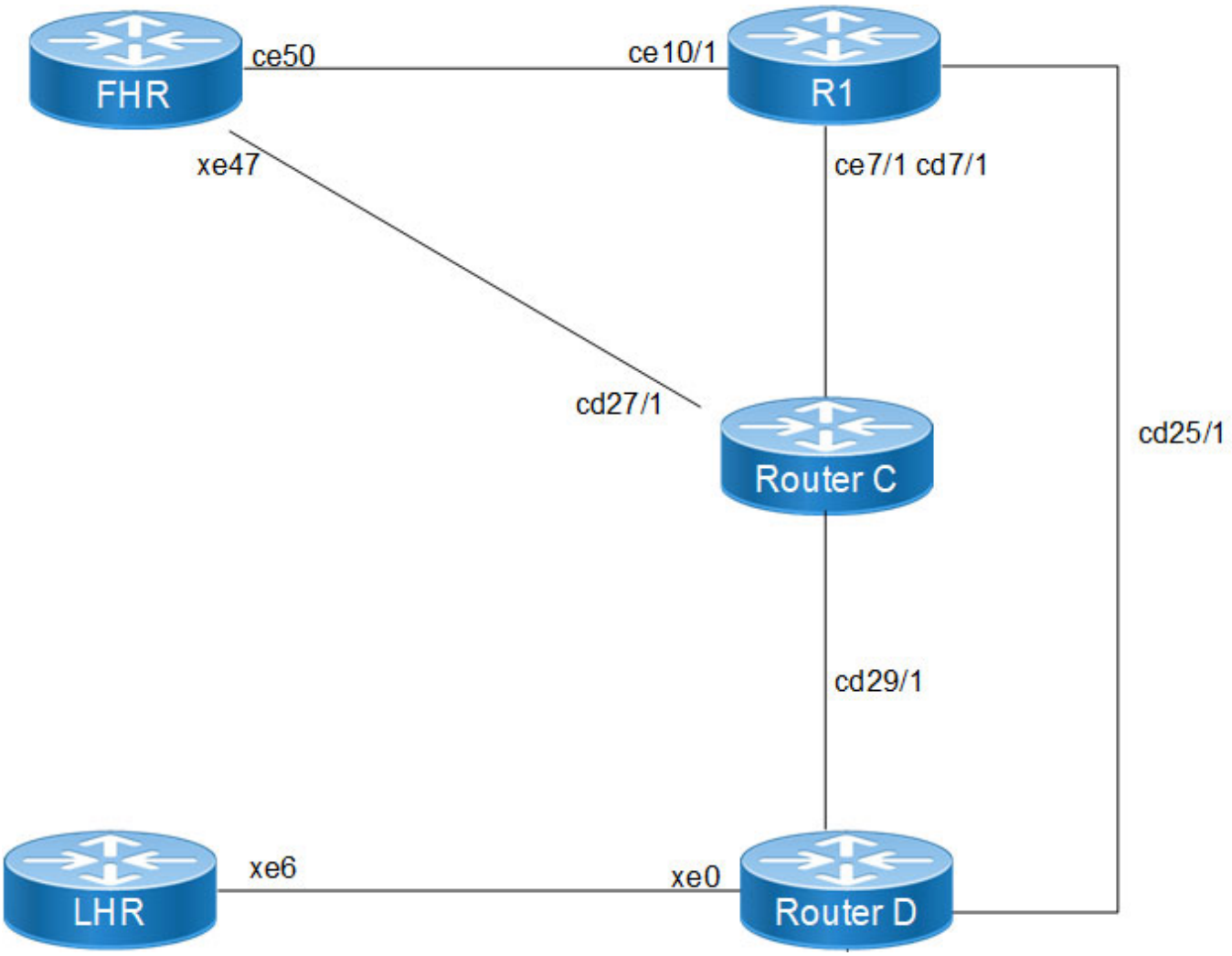
- IGP Connectivity: Routers must have reachability to the loopback addresses used for BSR and RP candidacy.

Configuration

BSR configurations apply to PIM-enabled routers within the Service Provider MPLS or IP network.

Topology

The PIM Bootstrap Router (BSR) topology is designed to support dynamic Rendezvous Point (RP) discovery across a multicast domain. It consists of five key OcNOS routers interconnected via physical board interfaces to manage multicast traffic flows between sources and receivers.



The following routers form the BSR domain, each performing a specific multicast function:

- First Hop Router: This node connects to the multicast source. It is responsible for encapsulating the source's data into PIM Register messages and sending them to the elected RP.
- Transit Node: A core router that provides a critical path between the source side (FHR) and the central multicast infrastructure.
- Candidate RP - Router_C: Configured as a Candidate RP (C-RP). It reports its candidacy to the BSR and, based on its priority (For example:priority 100), is elected to serve as the RP for a range of multicast groups.

- BSR & Candidate RP - Router_D: This node acts as the Candidate BSR (C-BSR). Once elected as the active BSR, it collects group-to-RP mappings from all C-RPs and broadcasts this information throughout the domain. It is also configured as a secondary C-RP.
- Last Hop Router: This node connects to the multicast receivers. It uses IGMP to learn about local receiver interest and then sends PIM Join messages toward the RP discovered via BSR messages.

Enable Multicast and PIM on All Nodes

1. Enable multicast routing and PIM sparse-mode on all interfaces across all routers in the domain to facilitate multicast traffic forwarding.

```
(config)# ip multicast-routing
(config)# ipv6 multicast-routing
(config-if)# ip pim sparse-mode
(config-if)# ipv6 pim sparse-mode
```

2. Configure Candidate BSR (on Router_D): Designate a router to participate in the BSR election. Configuring the priority allows for deterministic BSR selection; the highest priority value wins the election.

```
(config)# ip pim bsr-candidate lo 4 200
(config)# ipv6 pim bsr-candidate lo 4 200
```

3. Configure Candidate RP (on Router_C and Router_D): Identify routers that will serve as Rendezvous Points. Using a lower priority value ensures this node is preferred as the RP for the specified group range.

```
(config)# ip pim rp-candidate cd7/1 priority 100
(config)# ipv6 pim rp-candidate cd7/1 priority 100
```

Validation

Verify the dynamic RP and BSR status using the following show commands.

Verify BSR Information: Check which router has been elected as the BSR and its current priority.

```
LHR# show ip pim bsr-router
PIMv2 Bootstrap information
BSR address: 100.1.1.1
Uptime: 00:00:42, BSR Priority: 200, Hash mask length: 4
Role: Non-candidate BSR
State: Accept Preferred
```

For IPV6

```
#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 1001::1
  Uptime:      00:00:04, BSR Priority: 64, Hash mask length: 12
  Next bootstrap message in 00:00:03
  Role: Candidate BSR
  State: Elected BSR

  Candidate RP: 3001::2(xe47)
    Advertisement interval 4 seconds
    Next C-RP advertisement in 00:00:03
```

Verify Group-to-RP Mappings: Ensure the routers have learned the RP for specific multicast groups through the BSR mechanism.

```
LHR# show ip pim rp mapping
```

```
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 12.1.1.1
Info source: 100.1.1.1, via bootstrap, priority 100
```

For IPV6

```
# show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0


Group(s): ff00::/8, Static
    RP: 1001::1
         Uptime: 01:19:29
Embedded RP Groups:
```

Implementation Examples

Use Case: Large Enterprise Campus In a campus network with hundreds of VLANs, manually configuring a static RP on every access and distribution switch is error-prone. By implementing BSR, the administrator only needs to configure two core switches as C-BSRs and C-RPs. If the primary core switch fails, the BSR mechanism automatically promotes the secondary RP, ensuring uninterrupted video streaming or software distribution services.

Group to RP Mapping

Protocol Independent Multicast - Sparse Mode (PIM-SM) Group-to-Rendezvous Point (RP) mapping is a critical mechanism used in Any Source Multicast (ASM) domains to identify the RP for a specific multicast group. Each PIM-SM router maintains these mappings to determine how to join the shared tree for a group or where to send Register messages.

Feature Description

In a PIM-SM domain, routers learn the Group-to-RP mapping through various mechanisms such as Static RP, Auto-RP, or Bootstrap Router (BSR). OcNOS utilizes a defined algorithm to select the best RP from the available Group-to-RP mappings. This selection algorithm is designed to be consistent across the domain and does not prioritize based on the PIM mode or the specific mechanism (for example: Static vs. BSR) through which the mapping was learned.

Benefits

- Dynamic RP Discovery: Facilitates the automatic distribution of RP information throughout the PIM domain, reducing manual configuration overhead.
- Redundancy and Scalability: Supports multiple RP candidates and ensures all routers in the domain converge on the same RP for a specific group range.
- Flexible Group Management: Allows for granular control by mapping different multicast group ranges to different RPs.

Prerequisites

Before configuring Group-to-RP mappings, ensure the following base configurations are present on all participating routers:

- IP Multicast Routing: Multicast routing must be enabled globally on all PIM routers.
- PIM Sparse-Mode: PIM sparse-mode must be enabled on all transit and host-facing interfaces.
- Unicast Routing: A functional unicast routing protocol (for example: OSPF) must be configured to provide reachability between the LHR, FHR, and RP.

Configuration Prerequisites

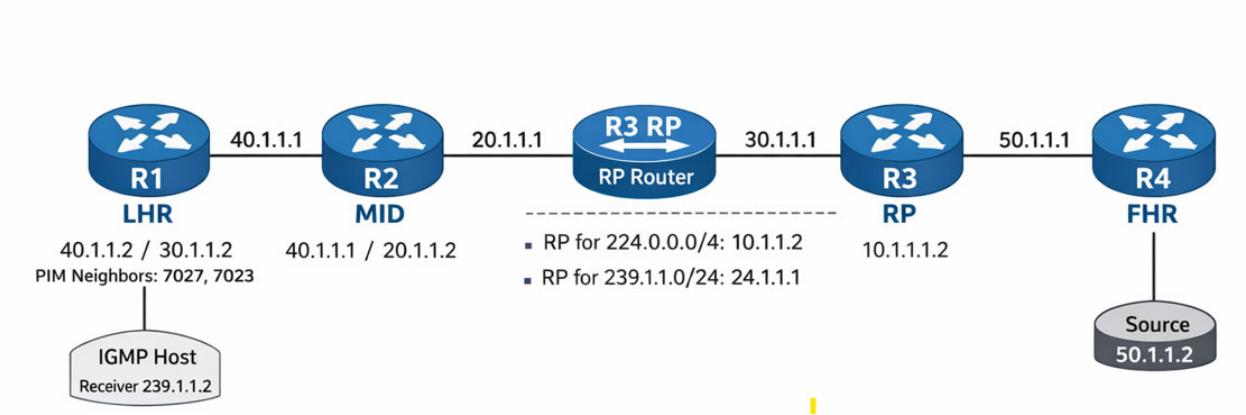
The following configurations should be set up to align with the topology:

- Configure OSPF to ensure reachability across the 10.1.1.0/24, 20.1.1.0/24, 30.1.1.0/24, 40.1.1.0/24, and 50.1.1.0/24 networks.
- Enable PIM sparse-mode on the relevant interfaces for R1 (LHR), R2 (MID), R3 (RP), and R4 (FHR).

Configuration

Configure various nodes within the topology to set up an PIM-SM Group-to-RP Mapping Scenario.

Topology



The topology consists of a linear path from the receiver to the source to demonstrate RP mapping and traffic flow.

- R1 (LHR): The Last Hop Router connected to the IGMP Host (Receiver 239.1.1.2).
- R2 (MID): A transit PIM router facilitating connectivity.
- R3 (RP): The Rendezvous Point for the domain, also acting as the Bootstrap Router (BSR).
- R4 (FHR): The First Hop Router connected to the Multicast Source (50.1.1.2).

Configuration Steps

The following PIM-SM Group-to-RP Mapping configurations apply to the RP and PIM-capable nodes within the Multicast network.

© 2026 IP Infusion Inc. Proprietary

1. Enable global multicast routing and configure the router to act as a BSR candidate and RP candidate for specific group lists to facilitate dynamic mapping distribution.

```
(config)# ip multicast-routing
(config)# ip pim bsr-candidate lo
(config)# ip pim rp-candidate lo group-list MC
(config)# ip pim rp-candidate xe1
```

2. On the LHR and transit nodes, enable PIM on interfaces and verify the learned mappings via the Bootstrap mechanism to ensure proper group-to-RP association.

```
(config)# interface xe4
(config-if)# ip pim sparse-mode
(config)# interface ce0
(config-if)# ip pim sparse-mode
```

Running Configurations

Here is the sample configuration for LHR:

```
!
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
!
ip vrf management
!
ip multicast-routing
!
ipv6 multicast-routing
!
interface cd1
!
interface cd3
!
interface ce0
ip address 40.1.1.2/24
ip pim sparse-mode
!
interface ce2
!
interface eth0
ip vrf forwarding management
ip address dhcp
!
interface lo
ip address 127.0.0.1/8
```

```
ipv6 address ::1/128
!
interface lo.management
ip vrf forwarding management
ip address 127.0.0.1/8
ipv6 address ::1/128
!
interface xe4
speed 10g
ip address 30.1.1.2/24

ipv6 address 3001::2/64
ipv6 router ospf area 0.0.0.0 instance-id 0
ip pim sparse-mode
ipv6 pim sparse-mode
!
interface xe5
!
interface xe18
ip address 60.1.1.1/24
ipv6 address 6001::1/64
ipv6 router ospf area 0.0.0.0 instance-id 0
ip pim sparse-mode
ipv6 pim sparse-mode
!
interface xe19
!

exit
!
router ospf 1
ospf router-id 5.5.5.5
network 5.5.5.5/32 area 0.0.0.0
network 10.1.1.0/24 area 0.0.0.0

network 30.1.1.0/24 area 0.0.0.0
network 40.1.1.0/24 area 0.0.0.0
network 60.1.1.0/24 area 0.0.0.0
!
router ipv6 ospf
router-id 1.1.1.1
!

port cd18 breakout 1X100g serdes 25g
port cd30 breakout 1X100g serdes 25g
port cd24 breakout 1X100g serdes 25g
port cd16 breakout 1X100g serdes 25g
port cd0 breakout 1X100g serdes 25g
tfo Disable
errdisable cause stp-bpdu-guard
```

© 2026 IP Infusion Inc. Proprietary

```
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
!
ip vrf management
!
ip multicast-routing
!
interface cd0/1
ip address 40.1.1.1/24
ip pim sparse-mode
!
interface cd1
!
interface cd2
!
interface cd3

!
interface cd4
!
interface cd5
!
!
interface cd16/1
ip address 20.1.1.2/24
ip pim sparse-mode
!
interface cd17
!

!
interface cd28
!
interface cd29
!
interface cd30/1
!
ip vrf forwarding management
ip address dhcp
!
interface lo
ip address 127.0.0.1/8
ipv6 address ::1/128
```

```
ipv6 pim sparse-mode
!
interface lo.management
ip vrf forwarding management
ip address 127.0.0.1/8
ipv6 address ::1/128
!
exit
!
router ospf 1
ospf router-id 1.1.1.1
network 20.1.1.0/24 area 0.0.0.0
network 40.1.1.0/24 area 0.0.0.0
!
line vty 0 16
exec-timeout 0 0
!
!
end
```

RP

```
!
qos enable
!
ip access-list standard MC
permit 239.1.1.0/24
!
ipv6 access-list standard MC1
permit ff03::/64

!
hostname rp
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
!
ip vrf management
!
ip multicast-routing
!
ipv6 multicast-routing
!
```

```
ip pim bsr-candidate lo
ip pim rp-candidate lo group-list MC
ip pim rp-candidate xe1
!
ipv6 pim bsr-candidate lo
ipv6 pim rp-candidate lo group-list MC1
ipv6 pim rp-candidate xe1
!
interface ce1
!
interface ce2

!
interface ce3
!
interface ce4
ip address 20.1.1.1/24
ip pim sparse-mode
!
interface ce5
!
interface ce6
!
interface ce7
!
interface ce8
!
interface ce9
!
interface ce10
!
interface ce23
!
ip vrf forwarding management
ip address dhcp
!
interface lo
ip address 127.0.0.1/8
ip address 24.1.1.1/24 secondary
ipv6 address ::1/128
ipv6 address 1111::1/64
ipv6 router ospf area 0.0.0.0 instance-id 0
ip pim sparse-mode
ipv6 pim sparse-mode
!
interface lo.management
ip vrf forwarding management
ip address 127.0.0.1/8
ipv6 address ::1/128
!
```

© 2026 IP Infusion Inc. Proprietary

```
interface xe0
!
interface xe1
speed 10g
ip address 10.1.1.2/24
ipv6 address 1001::2/64
ipv6 router ospf area 0.0.0.0 instance-id 0
ip pim sparse-mode
ipv6 pim sparse-mode
!
interface xe2
ip address 30.1.1.1/24
ipv6 address 3001::1/64
ipv6 router ospf area 0.0.0.0 instance-id 0

ip pim sparse-mode
ipv6 pim sparse-mode
!
interface xe3
!
exit
!
router ospf 1
ospf router-id 6.6.6.6
network 6.6.6.6/32 area 0.0.0.0
network 10.1.1.0/24 area 0.0.0.0
network 20.1.1.0/24 area 0.0.0.0
network 24.1.1.1/32 area 0.0.0.0
network 30.1.1.0/24 area 0.0.0.0
!
router ipv6 ospf
router-id 2.2.2.2
!
!
end
```

FHR

```
!
qos enable
!
hostname FHR
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
```

```
feature ntp vrf management
ntp enable vrf management
!
vlan database
vlan-reservation 4041-4094
!
ip vrf management

!
ip multicast-routing
!
ipv6 multicast-routing
!
interface ce49
!
interface ce50
!
interface ce51
!
interface ce52
!
interface ce53
!
interface ce54
!
interface eth0
ip vrf forwarding management
ip address dhcp
!
interface lo
ip address 127.0.0.1/8
ipv6 address ::1/128
!
interface lo.management
ip vrf forwarding management
ip address 127.0.0.1/8
ipv6 address ::1/128
!
interface xe1

!
interface xe2
!
interface xe3
!
interface xe4
!
interface xe23
ip address 50.1.1.1/24
ipv6 address 5001::1/64
```

```
ipv6 router ospf area 0.0.0.0 instance-id 0
ip pim sparse-mode
ipv6 pim sparse-mode
!
interface xe24
!
interface xe25

speed 10g
ip address 10.1.1.1/24
ipv6 address 1001::1/64
ipv6 router ospf area 0.0.0.0 instance-id 0
ipv6 mld version 2
ip pim sparse-mode
ipv6 pim sparse-mode
!

interface xe42
!
interface xe43

!
exit
!
router ospf 1
ospf router-id 8.8.8.8
network 6.6.6.6/32 area 0.0.0.0
network 8.8.8.8/32 area 0.0.0.0
network 10.1.1.0/24 area 0.0.0.0
network 30.1.1.0/24 area 0.0.0.0
network 50.1.1.0/24 area 0.0.0.0
!
router ipv6 ospf
router-id 3.3.3.3
!
!
end
```

Validation

Verify the PIM neighbor status on the LHR (R1)

```
LHR#show ip pim neighbor

Total number of PIM neighbors:2

Neighbor Interface Uptime/Expires Ver DR
Address Priority/Mode
40.1.1.1 ce0 00:02:05/00:01:36 v2 1 /
30.1.1.1 xe4 01:35:46/00:01:32 v2 1 /
```

Verify RP Mappings

Check the learned RP information on the LHR (R1). The output shows the group ranges and the associated RP addresses learned via BSR

```
LHR#show ip pim rp mapping

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 10.1.1.2
Info source: 24.1.1.1, via bootstrap, priority 192
Uptime: 00:16:55, expires: 00:01:35
Group(s): 239.1.1.0/24
RP: 24.1.1.1
Info source: 24.1.1.1, via bootstrap, priority 192
Uptime: 00:19:41, expires: 00:01:35
Override RP cnt: 0
LHR#sh ip igmp groups
IGMP Instance wide G-Recs Count is: 0
LHR#show ip igmp groups
IGMP Instance wide G-Recs Count is: 1
IGMP Connected Group Membership
Group Address Interface Uptime Expires State Last Reporte
r
239.1.1.2 xe18 00:00:01 00:04:17 Active 60.1.1.2

LHR#show ip igmp groups de
IGMP Instance wide G-Recs Count is: 1
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface: xe18
Group: 239.1.1.2
Flags: R
Uptime: 00:00:02
Group mode: Exclude (Expires: 00:04:17)
State: Active
Last reporter: 60.1.1.2

Source list is empty
```

Verify Multicast Route (mroute) Table

The RPF neighbor should point toward the RP.

```
LHR#show ip pim mr
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
```

```
(*, 239.1.1.2)
RP: 24.1.1.1
RPF nbr: 30.1.1.1
RPF idx: xe4
Upstream State: JOINED
Local ..i.............................
Joined ..............................
Asserted ............................
FCR:


LHR#show ip mr

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(50.1.1.2, 239.1.1.2), uptime 00:00:39, stat expires 00:02:52

Owner PIM, Flags: TF
Incoming interface: xe4
Outgoing interface list:
xe18 (1)

LHR#show ip pim mr
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1

(*, 239.1.1.2)
RP: 24.1.1.1
RPF nbr: 30.1.1.1
RPF idx: xe4
Upstream State: JOINED
Local ..i.............................
Joined ..............................
Asserted ............................
FCR:
Source: 50.1.1.2
Outgoing ..o..........................
KAT timer running, 168 seconds remaining
Packet count 1
```

Verify Traffic Rate

Confirm multicast traffic is flowing from the incoming interface to the outgoing interface connected to the receiver.

```
LHR# show interface counters rate mbps
+------------------+-------------+------------+-------------+-------------+

| Interface | Rx mbps | Rx pps | Tx mbps | Tx pps |
+------------------+-------------+------------+-------------+-------------+
xe4 20.85 39479 0.00 0
xe18 0.00 0 20.85 39481
```

Implementation Examples

Enterprise Multicast Isolation A corporation needs to separate internal training video traffic from general background multicast.

By configuring two different RPs and using BSR group-lists, the network engineer maps the training range (239.1.1.0/24) to a high-performance RP while keeping general traffic on a default RP. This optimizes traffic flow and provides administrative control over different multicast streams.

Anycast RP for IPv4 and IPv6

PIM Anycast Rendezvous Point (RP) is a networking solution designed to provide redundancy and load sharing for the RP in a Protocol Independent Multicast - Sparse Mode (PIM-SM) domain. By configuring multiple RPs with the same Anycast IP address, the network ensures high availability; if one RP fails, multicast traffic automatically reroutes to the topologically closest RP based on unicast routing metrics.

Feature Characteristics

- **Redundancy and Load Sharing:** Multiple RPs are configured with the same Anycast IP address, allowing the network to failover to a secondary RP if the primary becomes unreachable.
- **Dual-Stack Support:** Supports both IPv4 and IPv6 Anycast RP configurations.
- **MSDP-less Anycast:** Utilizes PIM anycast-rp commands to define the set of routers participating in the Anycast RP set, eliminating the need for Multicast Source Discovery Protocol (MSDP) in many scenarios.
- **Static RP Mapping:** Routers in the PIM domain use static configuration to point to the Anycast RP address.

Benefits

- **Efficient Traffic Control:** Multicast traffic follows the shortest path to the nearest available RP, reducing latency and network congestion.
- **Enhanced Reliability:** If one RP node fails, the underlying unicast routing protocol (e.g., OSPF) automatically redirects traffic to the next nearest RP node.
- **Scalability:** Simplifies the management of large multicast domains by providing a consistent RP address for all PIM-enabled routers.
- **Improved Performance:** Distributed RP load prevents a single router from becoming a bottleneck for multicast register messages and join requests.

© 2026 IP Infusion Inc. Proprietary

Configuration

Before configuring Anycast RP, ensure the following foundational protocols are active on all participating nodes:

- IP Multicast Routing: Must be enabled globally for both IPv4 and IPv6.
- Unicast Routing: OSPF or another IGP must be configured to provide reachability for the RP addresses and loopbacks.
- PIM Sparse-Mode: Enabled on all transit and host-facing interfaces.

Topology

The Anycast RP validation network is designed to demonstrate high availability and path optimization for both IPv4 and IPv6 multicast traffic across a service provider fabric. The topology is categorized into the following functional roles:

- FHR : This node serves as the entry point for multicast sources within the domain. It utilizes multiple paths to the core, specifically connecting to RP-1 via interface ce50 and the intermediate node via interface xe41.
- RP-1 : Functions as the primary Rendezvous Point for its topologically local segment. It is configured with a unique physical loopback 10.10.10.1 for peer synchronization and the shared Anycast RP address 10.10.10.10.
- RP-2 : Functions as a redundant Rendezvous Point, sharing the Anycast RP address 10.10.10.10. It provides load sharing and immediate failover capabilities should RP-1 become unreachable.
- Intermediate Transit Node : Acts as a core switching/routing element that maintains PIM neighbor relationships with the FHR, LHR, and both Anycast RPs. It ensures that Join/Prune messages are routed to the nearest available RP based on unicast IGP metrics.
- LHR : This node acts as the egress point for multicast subscribers and receivers. It manages IGMP/MLD group memberships on its host-facing interface xe18 and builds the shortest-path tree toward the Anycast RP address.

© 2026 IP Infusion Inc. Proprietary

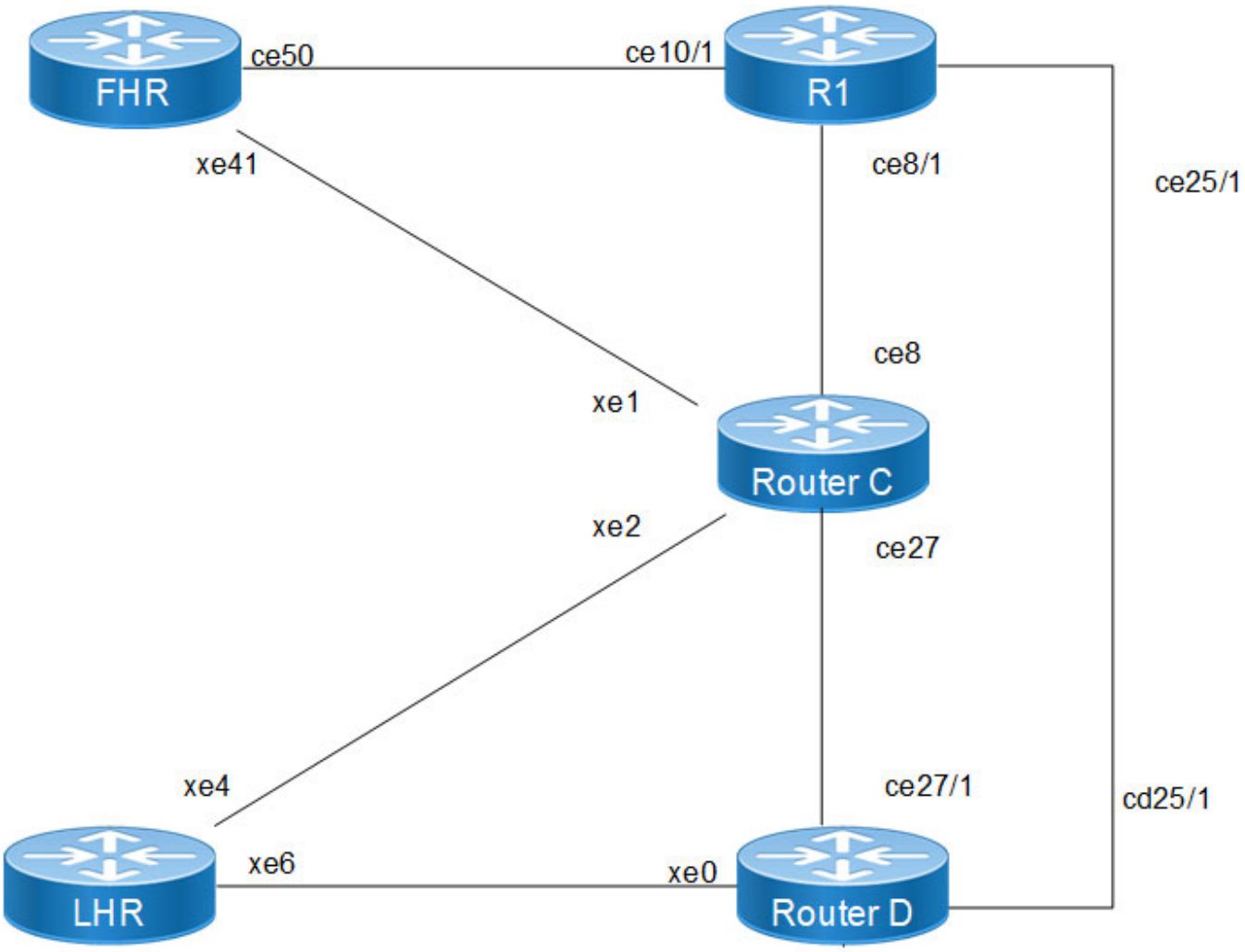


Figure 1-5: TAnycast RP Topology

The following PIM Anycast RP configurations applies to RP nodes and PIM domain routers within the OcNOS network.

1. Enable multicast routing globally on all routers to allow the processing of PIM join/prune messages and the maintenance of the multicast forwarding table.

```
(config)# ip multicast-routing
(config)# ipv6 multicast-routing
(config)# commit
```

2. Statically define the RP address on all routers in the PIM domain. This Anycast address (10.10.10.10 or 2001:db8:100::10) must be the same on every node to ensure a unified RP view.

```
(config)# ip pim rp-address 10.10.10.10
(config)# ipv6 pim rp-address 2001:db8:100::10
```

3. On the designated RP nodes, configure the Anycast RP membership. Each RP must list itself and its peers using its unique physical loopback addresses to facilitate register message synchronization.

```
(config)# ip pim anycast-rp 10.10.10.10 10.10.10.1
(config)# ip pim anycast-rp 10.10.10.10 10.10.10.2
(config)# ipv6 pim anycast-rp 2001:db8:100::10 2001:db8:100::1
(config)# ipv6 pim anycast-rp 2001:db8:100::10 2001:db8:100::2
```

© 2026 IP Infusion Inc. Proprietary

4. Configure the loopback interfaces on the RP nodes with both the unique physical address and the shared Anycast address to support PIM identification and reachability.

```
(config)# interface lo
(config-if)# ip address 10.10.10.1/32 secondary
(config-if)# ip address 10.10.10.10/32 secondary
(config-if)# ipv6 address 2001:db8:100::1/128
(config-if)# ipv6 address 2001:db8:100::10/128
(config-if)# ip pim sparse-mode
(config-if)# ipv6 pim sparse-mode
```

Validation

Verify the PIM Anycast RP configuration:

Verify RP Mapping and Anycast Members Use the `show ip pim rp mapping` command on the RP nodes to confirm the Anycast-RP members are correctly identified.

```
show ip pim rp mapping
PIM Group-to-RP Mappings
Anycast-RP  10.10.10.10 members :
10.10.10.1   10.10.10.2
Group(s): 224.0.0.0/4, Static
RP: 10.10.10.10
```

Verify PIM Neighbor States Ensure all routers have established PIM adjacencies over their respective interfaces.

```
show ip pim neighbor
Total number of PIM neighbors:4
Neighbor        Interface          Uptime/Expires            Ver   DR
190.1.1.1       xe2                00:37:23/00:01:23         v2    1
11.1.1.1        xe1                00:37:32/00:01:16         v2    1
```

Verify Multicast Routing Table (mroute) Check the mroute table on the LHR to ensure the (*, G) entries point toward the Anycast RP.

```
show ip pim mroute
(*, 225.1.1.1)
RP: 10.10.10.10
RPF nbr: 15.1.1.1
RPF idx: xe6
Upstream State: JOINED
```

Implementation Examples

Use Case: ISP Multicast Content Delivery An ISP providing IPTV services needs to ensure that the stream remains uninterrupted even if a core RP node fails. By deploying Anycast RP on two geographically separate routers, the ISP achieves automatic redundancy. Receivers will join via the topologically closest RP, optimizing bandwidth while providing a robust backup solution.

CHAPTER 2 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)

© 2026 IP Infusion Inc. Proprietary

- 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.

Similarly for ipv6, Source_1 address is 5001::2 and the group address is set to ff06::2.

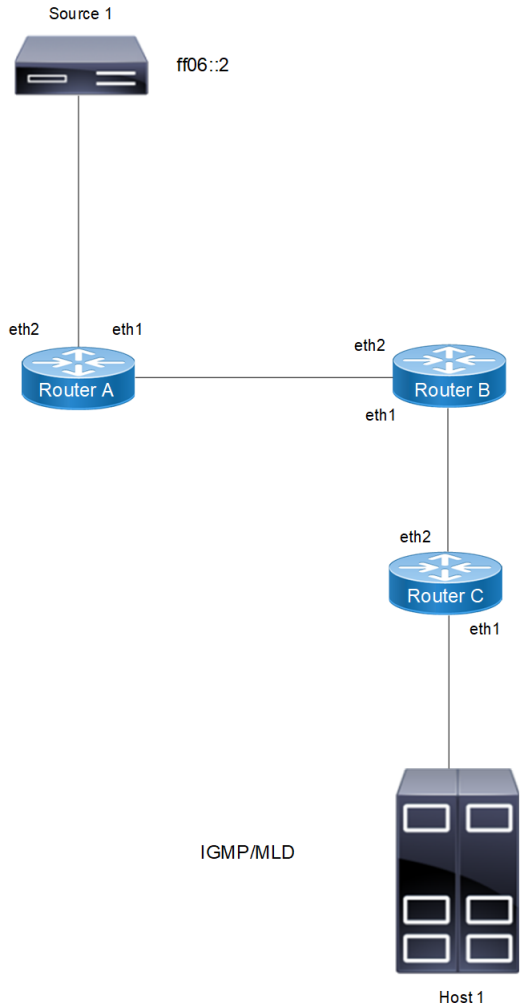


Figure 2-1: PIM-DM Configuration Topology

In this example, all routers are running PIM-DM.

1. Host_1 sends an IGMP/MLD 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/MLD 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(V4/V6) on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#commit`	Commit the transaction.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 multicast-routing`	Enable IPV6 multicast routing.
`(config)#commit`	Commit the transaction.

Enabling PIM-DM

Enable PIM-DM(V4/V6) 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)#commit`	Commit the transaction.
`(config-if)#end`	Enter the global configuration mode.
`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure the IPv6 address for eth1.
`(config-if)#ipv6 pim dense-mode`	Enable PIMv6 dense mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 3001::1/64`	Configure the IPv6 address for eth2.
`(config-if)#ipv6 pim dense-mode`	Enable PIMV6 dense mode on the interface.
`(config-if)#commit`	Commit the transaction.

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
!
For ipv6:
hostname Router_C
!
interface eth0
!
interface eth1
 ipv6 pim dense-mode
!
interface eth2
 ipv6 pim dense-mode
!
interface lo
!
!
Ipv6 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
```

Validation for ipv6-PIM-DM

The show ipv6 pim interface command displays the interface details for Router_C.

```
ROUTER_C#show ipv6 pim interface
Total number of PIM interfaces:2
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Prior
eth2       0        v2/D   1      1
    Address       : fe80::eac5:7aff:fea8:7cb9
    Global Address: 3001::1
eth1      1        v2/D   0      1
    Address       : fe80::eac5:7aff:fea8:7cc3
    Global Address: 2001::1
```

The show ipv6 mroute command displays the IPv6 multicast routing table.

```
ROUTER_C# show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface

(5001::2, ff06::2), uptime 00:00:15
Owner PIM, Flags: F
  Incoming interface: eth2
  Outgoing interface list:eth1
```

The show ipv6 pim mroute displays the IPV6 PIM-DM multicast routing table.

```
Router_C# show ipv6 pim mroute
PIM-DM Multicast Routing Table
(5001::2, ff06::2)
  RPF Neighbor: fe80::fa8e:a1ff:fe52:b247, Nexthop: fe80::fa8e:a1ff:fe52:b247, xe5
  Upstream IF: eth2
    Upstream State: Forwarding
    Upstream Prune Limit Timer Expiry: 0 secs
    Assert State: NoInfo
  Source Active Timer Expiry: 0 secs
  State Refresh Timer Expiry: 0 secs
  Downstream IF List:
```

```
eth1, in 'olist':
  Downstream State: NoInfo
  Assert State: NoInfo
```

Enable PIM-DM Sub-Interface

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)#bridge 1 protocol ieee vlan-bridge`	Configure the VLAN bridge
`(config)#vlan database`	Enter the VLAN database
`(config-vlan)#vlan 3-15 bridge 1 state enable`	Configure range of VLAN to bridge 1
`(config)#interface xe7.1`	Enter Interface mode.
`(config-if)#encapsulation dot1q 3`	Configure encapsulation dot1q
`(config-if)# ip address 10.1.1.2/24`	Configure the IP address for xe7.1.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface xe21.1`	Enter Interface mode.
`(config-if)#encapsulation dot1q 4`	Configure encapsulation dot1q
`(config-if)# ip address 11.1.1.1/24`	Configure the IP address for xe21.1.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#commit`	Commit the transaction.

Validation

The `show ip pim interface` command displays the interface details

```
DUT1#sh ip pim interface

Total number of PIM interfaces:2

Address          Interface   VIFindex   Ver/   Nbr    DR         DR
                                        Mode   Count  Prior
10.1.1.2         xe7.1       0          v2/D   1      1
11.1.1.1         xe21.1      1          v2/D   0      1
DUT1#
```

The `show ip mroute` command displays the IP multicast routing table.

```
DUT1#sh 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)

  (12.1.1.2, 231.1.1.1), uptime 00:00:15
  Owner PIM, Flags: F
    Incoming interface: xe7.1
    Outgoing interface list:
      Xe21.1 (1)
  DUT1#
```

The show ip pim mroute displays the IP PIM-DM multicast routing table.

```
  DUT1#sh ip pim mroute
  PIM-DM Multicast Routing Table
  (12.1.1.2, 231.1.1.1)
  RPF Neighbor: 10.1.1.1, Nexthop: 10.1.1.1, xe7.1
  Upstream IF: xe7.1
    Upstream State: Forwarding
    Upstream Prune Limit Timer Expiry: 0 secs
    Assert State: NoInfo
  Source Active Timer Expiry: 0 secs
  State Refresh Timer Expiry: 0 secs
  Downstream IF List:
    xe21.1:, in 'olist'
     Downstream State: NoInfo
     Assert State: NoInfo
```

CHAPTER 3 PIM-ECMP Redirect Configuration

A Protocol Independent Multicast (PIM) router uses Reverse Path Forwarding (RPF) procedure to select an upstream interface and router in order to build forwarding state. When there are equal-cost multipaths (ECMPs), existing implementations often use hash algorithms to select a path. Such algorithms do not allow the spread of traffic among the ECMPs according to administrative metrics. This usually leads to inefficient or ineffective use of network resources. PIM ECMP Redirect (RFC 6754) provides a mechanism to improve the RPF procedure over ECMPs. It allows ECMP selection to be based on administratively selected metrics, such as data transmission delays, path preferences, and routing metric. An interface identifier option is used in PIM hello messages as a tiebreaker during ECMP path selection.

Note: PIM ECMP Redirect is not supported for Bidirectional PIM, PIM-DM and PIM-SMDM.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-ECMP Redirect protocol:

Equal Cost Multipath (ECMP)

ECMP refers to parallel, single-hop, equal-cost links between adjacent nodes.

ECMP 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.

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.

Downstream

Away from the root of the multicast forwarding tree. A downstream router is a router that uses an interface in the ECMP bundle as an RPF interface for a multicast forwarding entry

When a PIM router downstream of the ECMP interfaces creates a new (*,G) or (S,G) entry, it will populate the RPF interface and RPF neighbor information according to the rules specified by [RFC4601]. This router will send its initial PIM Joins to that RPF neighbor. When the RPF neighbor router receives the Join message and finds that the receiving interface is one of the ECMP interfaces, it will check if the same flow is already being forwarded out of another ECMP interface. If so, this RPF neighbor router will send a PIM ECMPRedirect message onto the interface the Join was received on. The PIM ECMP Redirect message contains the address of the desired RPF neighbor, an Interface ID [RFC6395], and the other parameters used as tiebreakers. In essence, a PIM ECMP Redirect message is sent by an upstream router to notify downstream routers to redirect PIM Joins to the new RPF neighbor via a different interface. When the downstream routers receive this message, they SHOULD trigger PIM Joins toward the new RPF neighbor specified in the packet.

This PIM ECMP Redirect message has similar functions as the existing PIM Assert message:

- It is sent by an upstream router.

- It is used to influence the RPF selection by downstream routers.
- A tiebreaker metric is used

However, the existing Assert message is used to select an upstream router within the same multi-access network (such as a LAN), while the Redirect message is used to select both a network and an upstream router.

ECMP Redirect

ECMP Redirects are sent by an upstream router under either of the following conditions:

- It detects a PIM Join on a non-desired outgoing interface.
- It detects multicast traffic on a non-desired outgoing interface.

In both cases, an ECMP Redirect is sent to the non-desired interface. An outgoing interface is considered non-desired when:

- The upstream router is already forwarding the same flow out of another interface belonging to the same ECMP bundle.
- The upstream router is not yet forwarding the flow out any interfaces of the ECMP bundle, but there is another interface with more desired attributes.

Receiving ECMP Redirect

When a downstream router receives an ECMP Redirect, and detects that the desired RPF path from its upstream router's point of view is different from its current one, it should choose to join the newly suggested path and prune from the current path.

If a downstream router receives multiple ECMP Redirects sent by different upstream routers, it SHOULD use the Preference, Metric, or other fields as specified below as the tiebreakers to choose the most preferred RPF interface and neighbor. The tie-break procedure is the same as that used in PIM Assert processing described by [RFC4601].

If an upstream router receives an ECMP Redirect, it SHOULD NOT change its forwarding behavior even if the ECMP Redirect makes it a less preferred RPF neighbor on the receiving interface.

PIM-ECMP Configuration

This section provides the configuration steps for configuring PIM ECMP Redirect and examples for a relevant scenario.

Note: Configure PIM SM on the routers. For steps to configure PIM-SM refer to Chapter 1, *PIM Sparse Mode*

Topology

I

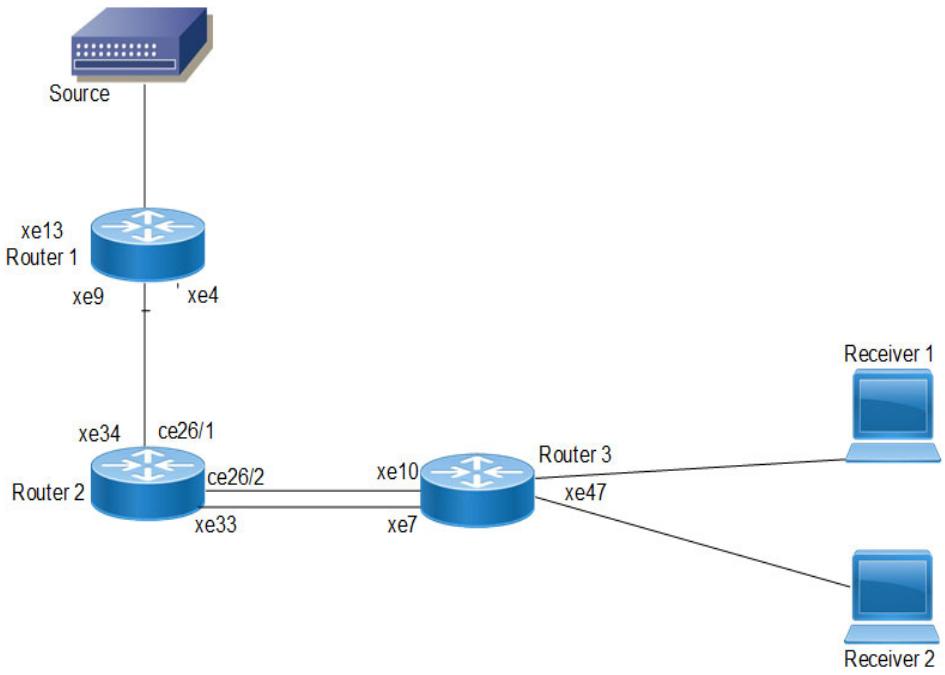


Figure 3-1: PIM ECMP Redirect Topology

Configure PIM ECMP Bundle

Configure PIM ECMP Bundle on all of the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# ip pim ecmp-bundle <bundle-name>`	Configure PIM ECMP Bundle
`(config)#exit`	Exit Configure mode.

Validation

```
#show running-config
!
ip multicast-routing
!
```

Bind PIM ECMP Bundle

Bind an ECMP Bundle to an interface on the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# interface eth1`	Enter Interface mode

`(config-if)# ip pim bind ecmp-bundle ecmpbundle`	Bind PIM ECMP Bundle to an interface
`(config-if)#exit`	Exit Interface mode.

Validation

Validation 1

Enter the commands listed in this section to confirm the previous configurations.

```
router_1#show running-config interface eth2
 interface eth2
 ip address 192.168.1.57/24
 no shutdown
 ip ospf cost 10
 ip pim bind ecmp-bundle ecmpbundle
 ip pim sparse-mode
 lldp-agent
 no dcbx enable
 exit
```

Validation 2

The following output displays the bundle information:

```
 router_1#show ip pim ecmp-bundle
Name         : ecmpbundle1
Interface    : <ECMP REDIRECT status>
       eth2 : allowed
       eth3 : allowed

router_1#show ip pim ecmp-bundle ecmpbundle1
Name        : ecmpbundle1
Interface    : <ECMP REDIRECT status>
       eth2 : allowed
       eth3 : allowed
 exit
```

Validation 3

The following output displays the interface details:

```
 router_1#show ip pim interface detail
  eth1 (vif 0):
  Address 192.168.10.57, Mode: Sparse
  DR 192.168.10.57, DR's priority: 1
  Hello period 30 seconds, Next Hello in 22 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 56e71c93
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.1 Local-ID 3
  Neighbors:
   192.168.10.52
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
```

```
PIM Neighbor policy: not configured

eth2 (vif 2):
Address 192.168.1.57, Mode: Sparse
DR 192.168.1.152, DR's priority: 1
Hello period 30 seconds, Next Hello in 23 seconds
Triggered Hello period 5 seconds
PIM GenID sent in Hellos: 5f2ebb37
Propagation delay is 1000 milli-seconds
Interface ID: Router-ID:1.1.1.1 Local-ID 4
ECMP REDIRECT, bundle : ecmpbundle1, status :  allowed
Neighbors:
 192.168.1.149
 192.168.1.150
 192.168.1.152
PIM neighbor count: 3
PIM neighbor holdtime: 105
PIM configured DR priority: 1
PIM border interface: no
PIM Neighbor policy: not configured
```

IP Multicast Routing Table for ECMP Redirect

Note: The multicast routing table displays for an RP router are different from other routers.

Validation 1:

Initially router_1 sends the (*, G) to Router_2 IF-2, as Router_2 IF-2 is RIB indicated RPF neighbor.The RIB indicated RPF neighbor can be checked using command `show ip rpf`

```
router_1#show ip rpf 172.31.5.153
RPF information for 172.31.5.153
  RPF interface: eth3
  RPF neighbor: 192.168.11.152
  RPF route: 172.31.5.0/24
  RPF type: unicast (ospf)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 110
  Metric: 30
```

Validation 2:

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr`	Displays the unicast next-hop to reach RP. and mask length.
`RPF idx`	Displays the incoming interface for this (*, G) state.
`RP`	Displays the IP address for the RP router
`B`	Displays the bidirectional PIM mode

`The leading dots....`

Stand for VIF index

Router-2 upon receiving (*, G) on IF-2, which is rib indicated RPF, sends an ECMP redirect message to Router-1 IF-2 to intimate that, subsequent joins should be sent to IF-1 being the desired path with a (*,G). Since, Router-2 IF-1 already has a (*, G), the `show ip pim mroute` command output suggests 192.168.1.152 as the RPF neighbor, which is ECMP redirected RPF neighbor.

```
router_1#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

(*, 224.1.1.1)
RP: 172.31.5.153
RPF nbr: 192.168.1.152
RPF idx: eth2
Upstream State: JOINED
 Local     i.............................
 Joined    .............................
 Asserted  .............................
FCR:
0
```

The below output displays (*,G) at router_2 IF-1 using the command `show ip pim mroute detail`:

```
router_2#show ip pim mroute detail
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.1.1.1) Uptime: 00:30:45
RP: 172.31.5.153, RPF nbr: 172.31.12.153, RPF idx: eth1
  Upstream:
   State: JOINED, SPT Switch: Disabled, JT Expiry: 15 secs
   Macro state: Join Desired,
  Downstream:
   eth1:
     State: JOINED, ET Expiry: 176 secs, PPT: off
     Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   eth1
  Join Olist:
   eth1
```

Configure PIM ECMP

Router-1 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config)#ip multicast-routing	Enable multi cast routing
(config)#ip pim ecmp-bundle redirect	Configure PIM ECMP Bundle
(config-if)#interface ce2	Enter the interface mode
(config-if)#ip address 50.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

Interface xe16

(config-if)#interface xe16	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 10.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

interface xe17

(config-if)#interface xe17	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 20.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode
(config-if)#router ospf 1	Configure OSPF
(config-if)#ospf router-id 3.3.3.3	Configure OSPF router id
(config-if)#network 3.3.3.3/32 area 0.0.0.0	Configure OSPF network id
(config-if)#network 10.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 20.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 50.1.1.0/24 area 0.0.0.0	Configure OSPF network id

Router-2 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config)#ip multicast-routing	Enable multi cast routing
(config)#ip pim ecmp-bundle redirect	Configure PIM ECMP Bundle
(config-if)#interface ce2	Enter the interface mode

(config-if)#ip address 50.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

Interface xe16

(config-if)#interface xe16	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 10.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

Interface xe17

(config-if)#interface xe17	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 20.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode
(config-if)#router ospf 1	Configure OSPF
(config-if)#ospf router-id 3.3.3.3	Configure OSPF router id
(config-if)#network 3.3.3.3/32 area 0.0.0.0	Configure OSPF network id
(config-if)#network 10.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 20.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 50.1.1.0/24 area 0.0.0.0	Configure OSPF network id

Router-3 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config)#ip multicast-routing	Enable multi cast routing
(config)#ip pim ecmp-bundle redirect	Configure PIM ECMP Bundle
(config-if)#interface ce2	Enter the interface mode
(config-if)#ip address 50.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

Interface xe16

(config-if)#interface xe16	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 10.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode

Interface xe17

(config-if)#interface xe17	Enter the interface mode
(config-if)#speed 10g	Configure interface speed same as peer interface
(config-if)#ip address 20.1.1.2/24	Configure IPv4 address
(config-if)#ip pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)#ip pim sparse-mode	Configure multi cast sparse mode
(config-if)#router ospf 1	Configure OSPF
(config-if)#ospf router-id 3.3.3.3	Configure OSPF router id
(config-if)#network 3.3.3.3/32 area 0.0.0.0	Configure OSPF network id
(config-if)#network 10.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 20.1.1.0/24 area 0.0.0.0	Configure OSPF network id
(config-if)#network 50.1.1.0/24 area 0.0.0.0	Configure OSPF network id

Validation-1

The following output displays the bundle information.

```
OcNOS#show ip pim ecmp-bundle
Name        : redirect
Interface   : <ECMP REDIRECT status>
        ce2 : allowed
       xe16 : allowed
       xe17 : allowed
```

Validation-2

The following output displays the interface details.

```
OcNOS#show ip pim ecmp-bundle
Name        : redirect
Interface   : <ECMP REDIRECT status>
        ce2 : allowed
       xe16 : allowed
       xe17 : allowed
OcNOS#show ip pim interface detail
ce2 (vif 0):
  Address 50.1.1.2, Mode: Sparse
  DR 50.1.1.2, DR's priority: 1
  Hello period 30 seconds, Next Hello in 12 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 7b030d86
  Propagation delay is 500 milli-seconds
```

```
  Interface ID: Router-ID:50.1.1.2 Local-ID 10017
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Neighbors:
  PIM neighbor count: 0
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

xe16 (vif 2):
  Address 10.1.1.2, Mode: Sparse
  DR 10.1.1.3, DR's priority: 1
  Hello period 30 seconds, Next Hello in 15 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 2f97be24
  Propagation delay is 500 milli-seconds
  Interface ID: Router-ID:50.1.1.2 Local-ID 10037
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Neighbors:
   10.1.1.3
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

xe17 (vif 3):
  Address 20.1.1.2, Mode: Sparse
  DR 20.1.1.3, DR's priority: 1
  Hello period 30 seconds, Next Hello in 16 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 44982df7
  Propagation delay is 500 milli-seconds
  Interface ID: Router-ID:50.1.1.2 Local-ID 10038
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Neighbors:
   20.1.1.3
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured
```

Validation-3

Initially router_1 sends the (*, G) to Router_2 IF-2, as Router_2 IF-2 is RIB indicated RPF neighbor. The RIB indicated RPF neighbor can be checked using command show ip rpf

IP Multi cast Routing Table for ECMP Redirect

```
OcNOS#show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface
(239.1.1.1), uptime 00:10:47, stat expires 00:01:52
```

```
Owner PIM, Flags: TF
  Incoming interface: xe34
  Outgoing interface list:
    xe33 (1)

OcNOS#show ipv6 pim mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
(5001::2, ff06::1)
RPF nbr: fe80::eac5:7aff:fe0a:8533
RPF idx: xe34
SPT bit: 1
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
 Outgoing  o..............................
(239.1.1.2::1, rpt)
RP: ::
RPF nbr: ::
RPF idx: None
Upstream State: RPT NOT JOINED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..............................
```

PIM-IPv6-ECMP Redirect Configuration

Router-1 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config-vlan)vlan 10 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 20 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 50 bridge 1 state enable	Configure VLAN
(config)#ipv6 multicast-routing	Enable IPv6 multi cast routing
(config)#ipv6 pim ecmp-bundle redirect	Create ECMP bundle group
(config)#ipv6 pim ecmp-bundle redirect	Configure multi cast sparse mode
(config-if)interface vlan1.10	Enter VLAN interface mode
(config-if)ipv6 address 7001::1/64	Configure IPv6 interface
(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
(config-if)interface vlan1.20	Enter the VLAN interface mode
(config-if)ipv6 address 4001::2/64	Configure IPv6 interface
(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure IPv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 pim sparse mode
(config-if)interface vlan1.50	Enter VLAN interface mode
(config)ipv6 address 5001::1/64	Configure IPv6 interface
(config)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config)ipv6 mld version 2 ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group

© 2026 IP Infusion Inc. Proprietary

Router-2 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config-vlan)vlan 10 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 20 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 50 bridge 1 state enable	Configure VLAN
(config)#ipv6 multicast-routing	Enable IPv6 multi cast routing
(config)#ipv6 pim ecmp-bundle redirect	Create ECMP bundle group
(config-if)interface vlan1.10	Enter VLAN interface mode
(config-if)ipv6 address 7001::1/64	Configure IPv6 interface
(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
(config-if)interface vlan1.20	Enter the VLAN interface mode
(config-if)ipv6 address 4001::2/64	Configure IPv6 interface
(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure IPv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 pim sparse mode
(config-if)interface vlan1.50	Enter VLAN interface mode
(config)ipv6 address 5001::1/64	Configure IPv6 interface
(config)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config)ipv6 mld version 2 ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group

Router-3 Config

(config)#bridge 1 protocol ieee vlan-bridge	Create VLAN bridge
(config)#vlan database	Enter VLAN database
(config-vlan)vlan 10 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 20 bridge 1 state enable	Configure VLAN
(config-vlan)vlan 50 bridge 1 state enable	Configure VLAN
(config)#ipv6 multicast-routing	Enable IPv6 multi cast routing
(config)#ipv6 pim ecmp-bundle redirect	Create ECMP bundle group
(config-if)interface vlan1.10	Enter VLAN interface mode
(config-if)ipv6 address 7001::1/64	Configure IPv6 interface

(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
(config-if)interface vlan1.20	Enter the VLAN interface mode
(config-if)ipv6 address 4001::2/64	Configure IPv6 interface
(config-if)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure IPv6 OSPF area and instance id
(config-if)ipv6 mld version 2	Create MLD version
(config-if)ipv6 pim bind ecmp-bundle redirect	Bind ECMP bundle group
(config-if)ipv6 pim sparse-mode	Configure IPv6 pim sparse mode
(config-if)interface vlan1.50	Enter VLAN interface mode
(config)ipv6 address 5001::1/64	Configure IPv6 interface
(config)ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0	Configure ipv6 OSPF area and instance id
(config)ipv6 mld version 2 ipv6 pim bind ecmp-bundle redirect	Bind CECMP bundle group

Validation-1

Enter the commands listed in this section to confirm the previous configurations.

```
show  running-config interface
interface vlan1.10
ipv6 address 7001::1/64
ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0
ipv6 mld version 2
ipv6 pim bind ecmp-bundle redirect
ipv6 pim sparse-mode
!
interface vlan1.20
ipv6 address 4001::2/64
ipv6 router ospf area 0.0.0.0 tag 100 instance-id 0
ipv6 mld version 2
ipv6 pim bind ecmp-bundle redirect
ipv6 pim sparse-mode
```

Validation 2

The following output displays the bundle information.

```
show ipv6 pim ecmp-bundle
Name        : redirect
Interface   : <ECMP REDIRECT status>
   vlan1.50 : allowed
   vlan1.20 : allowed
   vlan1.10 : allowed
```

Validation 3

The following output displays the interface details.

```
show ipv6 pim interface detail
vlan1.10 (vif 3):
  Address fe80::eac5:7aff:fe25:f131, Mode: Sparse
  DR fe80::eac5:7aff:fe25:f131, DR's priority: 1
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 1eddc141
  Propagation delay is 500 milli-seconds
  Interface ID: Router-ID:0.0.0.0 Local-ID 10059
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Secondary addresses:
   7001::1
  Neighbors:
   fe80::36ef:b6ff:fe94:3db4
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

vlan1.20 (vif 2):
  Address fe80::eac5:7aff:fe25:f131, Mode: Sparse
  DR fe80::eac5:7aff:fe25:f131, DR's priority: 1
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 7b93f3a0
  Propagation delay is 500 milli-seconds
  Interface ID: Router-ID:0.0.0.0 Local-ID 10069
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Secondary addresses:
   4001::2
  Neighbors:
   fe80::36ef:b6ff:fe94:3db4
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

vlan1.50 (vif 0):
  Address fe80::eac5:7aff:fe25:f131, Mode: Sparse
  DR fe80::eac5:7aff:fe25:f131, DR's priority: 1
  Hello period 30 seconds, Next Hello in 12 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 4dae86d7
  Propagation delay is 500 milli-seconds
  Interface ID: Router-ID:0.0.0.0 Local-ID 10099
  ECMP REDIRECT, bundle : redirect, status :  allowed
  Secondary addresses:
   5001::1
  Neighbors:
  PIM neighbor count: 0
  PIM configured DR priority: 1
```

```
  PIM border interface: no
  PIM Neighbor policy: not configured
```

Validation 4

Initially router_1 sends the (*, G) to Router_2 IF-2, as Router_2 IF-2 is RIB indicated RPF neighbor.The RIB indicated RPF neighbor can be checked using command `show ip rpf`

```
show ipv6 rpf 4001::2
RPF information for 4001::2
  RPF interface: vlan1.20
  RPF neighbor: ::
  RPF route: 4001::/64
  RPF type: unicast (connected)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
```

CHAPTER 4 PIM-BFD Configuration

PIM is a multicast routing protocol which uses Hello messages to detect adjacent node failure. This mechanism is very slow and leads to control plane overhead when interval between hello messages is set to minimum.

BFD is a protocol designed to detect link failures superfast, routing protocols such as OSPF, ISIS uses BFD to get link failure notification.

BFD detects the link failure immediately after the original DR fails and triggers new DR election. The BFD protocol uses control packets and shorter detection time limits to more rapidly detect failures in a network.

Topology

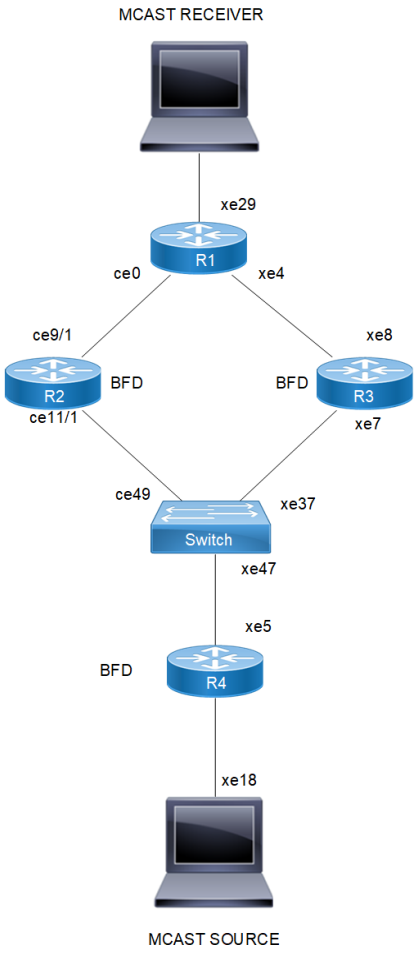


Figure 4-1: PIM-BFD Configuration Topology

PIM-BFD Configuration

This document captures requirements to use BFD with PIM IPv4 and IPv6 to detect adjacent neighbor reachability failure.

Note: IPv6 PIM is supported in Qumran2 series platforms.

R1

`#configure terminal`	Enter configuration mode.
`OcNOS(config)#ip multicast-routing`	Configure IP multicast routing
`OcNOS(config)#ipv6 multicast-routing`	Configure IPv6 multicast routing
`OcNOS(config)#interface xe29`	Entering in to interface
`OcNOS(config-if)#ipv6 address 5001::1/64`	Configure IPv6 address
`OcNOS(config-if)#ip address 14.14.14.1/24`	Configure IPv4 address
`OcNOS(config-if)#ip pim sparse-mode`	Configure PIM sparse mode
`OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0`	Configure OSPF to interface
`OcNOS(config-if)#ipv6 pim sparse-mode`	Configure IPv6 PIM sparse mode
`OcNOS(config-if)#commit`	Commit all the transactions
`OcNOS(config)#interface ce0`	Entering in to interface
`OcNOS(config-if)#ipv6 address 2001::1/64`	Configure IPv6 address
`OcNOS(config-if)#ip address 12.12.12.1/24`	Configure IP address
`OcNOS(config-if)#ip pim sparse-mode`	Configure PIM sparse mode
`OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0`	Configure OSPF to interface
`OcNOS(config-if)#ipv6 pim sparse-mode`	Configure IPv6 PIM sparse mode
`OcNOS(config-if)#commit`	Commit all the transactions
`OcNOS(config-if)#exit`	Exit
`OcNOS(config)#interface xe4`	Entering in to interface
`OcNOS(config-if)#ipv6 address 3001::1/64`	Configure IPv6 address
`OcNOS(config-if)#ip address 13.13.13.1/24`	Configure IP address
`OcNOS(config-if)#ip pim sparse-mode`	Configure PIM sparse mode
`OcNOS(config-if)# ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0`	Configure OSPF to interface
`OcNOS(config-if)#ipv6 pim sparse-mode`	Configure IPv6 PIM sparse mode
`OcNOS(config-if)#commit`	Commit all the transactions
`OcNOS(config-if)#exit`	Exit
`OcNOS(config)#router ospf 1`	Configure IP OSPF
`OcNOS(config-router)#ospf router-id 20.20.20.1`	Configure router id under ospf
`OcNOS(config-router)#network 12.12.12.0/24 area 0.0.0.0`	Add network under OSPF
`OcNOS(config-router)#network 13.13.13.0/24 area 0.0.0.0`	Add network under OSPF
`OcNOS(config-router)#network 14.14.14.0/24 area 0.0.0.0`	Add network under OSPF
`OcNOS(config-router)#network 20.20.20.1/32 area 0.0.0.0`	Add network under OSPF
`OcNOS(config)#router ipv6 ospf 1`	Configure IPv6 OSPF
`OcNOS(config-router)#router-id 1.1.1.1`	Configure router ID under OSPF

OcNOS(config-router)#commit	Commit all the transactions
OcNOS(config)#exit	Exit

R2

#configure terminal	Enter configuration mode.
OcNOS(config)#bridge 1 protocol mstp	Configure bridge 1 protocol MSTP/IEEE VLAN bridge
OcNOS(config)#vlan database	Entering in to VLAN database
OcNOS(config-vlan)#vlan 120 bridge 1 state enable	Configure VLAN 120 with bridge 1 state enable
OcNOS(config-vlan)#ip multicast-routing	Configure IP multicast routing
OcNOS(config-vlan)#ipv6 multicast-routing	Configure IPv6 multicast routing
OcNOS(config)#interface vlan1.120	Entering VLAN interface
OcNOS(config-if)#ipv6 address 1001::2/64	Configure IPv6 address
OcNOS(config-if)#ip address 10.10.10.2/24	Configure IP address
OcNOS(config-if)#ip pim sparse-mode	Configure PIM sparse mode
OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0	Configure OSPFv6
OcNOS(config-if)#ipv6 pim bfd	Configure IPv6 PIM BFD
OcNOS(config-if)#ip pim bfd	Configure IP BFD
OcNOS(config-if)#ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
OcNOS(config-if)#commit	Commit all the transactions
OcNOS(config-if)#exit	Exit
OcNOS(config)#ipv6 pim bsr-candidate vlan1.120	Configure IPv6 PIM BSR candidate
OcNOS(config)#commit	Commit all the transactions
OcNOS(config)#interface ce11/1	Entering interface ce7/1
OcNOS(config-if)#switchport	Configure Switchport
OcNOS(config-if)#bridge-group 1	Configure bridge group1
OcNOS(config-if)#switchport mode access	Configure switchport mode access
OcNOS(config-if)#switchport access vlan 120	Configure switchport access mode
OcNOS(config-if)#commit	Commit all the transactions
OcNOS(config-if)#interface ce9/1	Entering interface ce9/1
OcNOS(config-if)#ipv6 address 2001::2/64	Configure IPv6 address
OcNOS(config-if)#ip address 12.12.12.2/24	Configure IP address
OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0	Configure OSPFv6 under interface
OcNOS(config-if)#ip pim sparse-mode	Configure PIM sparse mode
OcNOS(config-if)#ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
OcNOS(config-if)#commit	Commit all the transactions
OcNOS(config-if)#exit	Exit
OcNOS(config)#router ospf 1	Configure IP OSPF

OcNOS(config-router)#ospf router-id 20.20.20.2	Configure router ID under ospf
OcNOS(config-router)#network 10.10.10.0/24 area 0.0.0.0	Add network under OSPF
OcNOS(config-router)#network 12.12.12.0/24 area 0.0.0.0	Add network under OSPF
OcNOS(config-router)#network 20.20.20.2/32 area 0.0.0.0	Add network under OSPF
OcNOS(config)#router ipv6 ospf 1	Configure IPv6 OSPF
OcNOS(config-router)#router-id 2.2.2.2	Configure router ID under OSPF
OcNOS(config-router)#commit	Commit all the transactions
OcNOS(config-if)#exit	Exit

R3

#configure terminal	Enter configuration mode.
OcNOS(config)#bridge 1 protocol mstp	Configure bridge 1 protocol MSTP/IEEE VLAN bridge
OcNOS(config)#vlan database	Entering in to VLAN database
OcNOS(config-vlan)#vlan 120 bridge 1 state enable	Configure VLAN 120 with bridge 1 state enable
OcNOS(config-vlan)#ip multicast-routing	Configure IP multicast routing
OcNOS(config-vlan)#ipv6 multicast-routing	Configure IPv6 multicast routing
OcNOS(config)#interface vlan1.120	Entering VLAN interface
OcNOS(config-if)#ipv6 address 1001::3/64	Configure IPv6 address
OcNOS(config-if)#ip address 10.10.10.2/24	Configure IP address
OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0	Configure OSPFv6
OcNOS(config-if)#ip pim sparse-mode	Configure PIM sparse mode
OcNOS(config-if)#ip pim bfd	Configure PIM BFD
OcNOS(config-if)#ipv6 pim bfd	Configure IPv6 PIM BFD
OcNOS(config-if)#ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
OcNOS(config-if)#commit	Commit all the transactions
OcNOS(config-if)#exit	Exit
OcNOS(config)#ipv6 pim bsr-candidate vlan1.120	Configure IPv6 PIM BSR candidate
OcNOS(config)#commit	Commit all the transactions
OcNOS(config)#interface xe7	Entering interface ce7/1
OcNOS(config-if)#switchport	Configure Switchport
OcNOS(config-if)#bridge-group 1	Configure bridge group1
OcNOS(config-if)#switchport mode access	Configure switchport mode access
OcNOS(config-if)#switchport access vlan 120	Configure switchport access mode
OcNOS(config-if)#commit	Commit all the transactions
OCNOS(config)#interface xe8	Entering interface
OCNOS(config-if)#ipv6 address 3001::2/64	Configure IPv6 address

OCNOS(config-if)#ip address 13.13.13.2/24	Configure IP address
OCNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0	Configure OSPFv6 under interface
OCNOS(config-if)#ipv6 pim sparse-mode	Configure IPv6 PIM sparse mode
OCNOS(config-if)#ip pim sparse-mode	Configure IP PIM sparse mode
OCNOS(config-if)#commit	Commit all the transactions
OCNOS(config-if)#exit	Exit
OcNOS(config)#router ospf 1	Configure IP OSPF
OcNOS(config-router)#ospf router-id 20.20.20.3	Configure router id under OSPF
OcNOS(config-router)#network 10.10.10.0/24 area 0.0.0.0	Add network under OSPF
OcNOS(config-router)#network 13.13.13.0/24 area 0.0.0.0	Add network under OSPF
OcNOS(config-router)#network 20.20.20.3/32 area 0.0.0.0	Add network under OSPF
OcNOS(config)#router ipv6 ospf 1	Configure IPv6 OSPF
OcNOS(config-router)#router-id 3.3.3.3	Configure router id under OSPF
OcNOS(config-router)#commit	Commit all the transactions
OCNOS(config-if)#exit	Exit

SWITCH

#configure terminal	Enter configuration mode.
(config)#bridge 1 protocol mstp	Bridge config
OcNOS(config)#vlan database	Entering in to VLAN database
OcNOS(config-vlan)#vlan 120 bridge 1 state enable	Configure VLAN 120 with bridge 1 state enable
OcNOS(config-if)#interface ce49	Entering interface xe1
OcNOS(config-if)#switchport	Configure Switchport
OcNOS(config-if)#bridge-group 1	Configure bridge group1
OcNOS(config-if)#switchport mode access	Configure switchport mode access
OcNOS(config-if)#switchport access vlan 120	Configure switchport access mode
OcNOS (config-if)#exit	Exit interface mode.
OcNOS(config-if)#interface xe37	Entering interface xe1
OcNOS(config-if)#switchport	Configure Switchport
OcNOS(config-if)#bridge-group 1	Configure bridge group1
OcNOS(config-if)#switchport mode access	Configure switchport mode access
OcNOS(config-if)#switchport access vlan 120	Configure switchport access mode
OcNOS (config-if)#exit	Exit interface mode.
OcNOS(config-if)#interface xe47	Entering interface xe1
OcNOS(config-if)#switchport	Configure Switchport
OcNOS(config-if)#bridge-group 1	Configure bridge group1

`OcNOS(config-if)#switchport mode access`	Configure switchport mode access
`OcNOS(config-if)#switchport access vlan 120`	Configure switchport access mode
`OcNOS (config-if)#exit`	Exit interface mode.
`OcNOS(config-if)#commit`	Commit all the transactions

R4

`#configure terminal`	Enter configuration mode.
`OcNOS(config)#ipv6 multicast-routing`	Configure IPv6 multicast routing
`OcNOS(config)#ip multicast-routing`	Configure IP multicast routing
`OcNOS(config)#interface xe18`	Entering in to interface
`OcNOS(config-if)#ipv6 address 6001::1/64`	Configure IPv6 address
`OcNOS(config-if)#ip address 16.16.16.1/24`	Configure IP address
`OcNOS(config-if)#ipv6 mld version 2`	Configure MLD version 2
`OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0`	Configure OSPF to interface
`OcNOS(config-if)#ip pim sparse-mode`	Configure PIM sparse mode
`OcNOS(config-if)#ipv6 pim sparse-mode`	Configure IPv6 PIM sparse mode
`OcNOS(config-if)#commit`	Commit all the transactions
`OcNOS(config)#interface xe5`	Entering in to interface
`OcNOS(config-if)#ipv6 address 1001::1/64`	Configure IPv6 address
`OcNOS(config-if)#ip address 10.10.10.1/24`	Configure IP address
`OcNOS(config-if)#ipv6 router ospf area 0.0.0.0 tag 1 instance-id 0`	Configure OSPF to interface
`OcNOS(config-if)#ip pim sparse-mode`	Configure PIM sparse mode
`OcNOS(config-if)#ipv6 pim sparse-mode`	Configure IPv6 PIM sparse mode
`OcNOS(config-if)#ip pim bfd`	Configure IP PIM BFD
`OcNOS(config-if)#ipv6 pim bfd`	Configure IPv6 PIM BFD
`OcNOS(config-if)#commit`	Commit all the transactions
`OcNOS(config-if)#exit`	Exit
`OcNOS(config)#router ospf 1`	Configure IP OSPF
`OcNOS(config-router)#ospf router-id 20.20.20.4`	Configure router id under OSPF
`OcNOS(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add network under OSPF
`OcNOS(config-router)#network 16.16.16.0/24 area 0.0.0.0`	Add network under OSPF
`OcNOS(config-router)#network 20.20.20.4/32 area 0.0.0.0`	Add network under OSPF
`OcNOS(config)#router ipv6 ospf 1`	Configure IPv6 OSPF
`OcNOS(config-router)#router-id 5.5.5.5`	Configure router id under OSPF
`OcNOS(config-router)#commit`	Commit all the transactions
`OcNOS(config)#exit`	Exit

Validation

R1

```
#show ipv6 pim neighbor

Total number of PIM neighbors:2

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::36ef:b6ff:fe94:3df5                 ce0         00:00:38/00:01:24 1 /
fe80::e201:a6ff:fe4b:f30a                 xe4         00:00:41/00:01:30 1 /

#show ip pim neighbor

Total number of PIM neighbors:2

Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
12.12.12.2      ce0                00:11:17/00:01:28         v2    1 / DR
13.13.13.2      xe4                00:11:19/00:01:27         v2    1 / DR
```

R2

```
#show ipv6 pim neighbor

Total number of PIM neighbors:3

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::eac5:7aff:feb1:6b11                 ce9/1       00:12:51/00:01:24 1 / DR
fe80::e201:a6ff:fe4b:f301                 vlan1.120   00:02:28/00:01:17 1 /
fe80::eac5:7aff:fe78:a2cc                 vlan1.120   00:02:28/00:01:29 1 / DR

#show ip pim neighbor

Total number of PIM neighbors:3

Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
12.12.12.1      ce9/1              00:09:15/00:01:32         v2    1 /
10.10.10.1      vlan1.120          00:09:44/00:01:31         v2    1 /
10.10.10.3      vlan1.120          00:10:56/00:01:20         v2    1 / DR

#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
258       NA          IPv6       Micro-BFD   Up         00:34:25  vlan1.120     NA
fe80::eac5:7aff:fea8:7cb9/128
```

```
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
           Single Hop  ce11/1         2         2056       Up

259      NA         IPv4       Micro-BFD  Up        00:23:03  vlan1.120     NA
10.10.10.1/32
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
           Single Hop  ce11/1         3         4          Up

257      NA         IPv4       Micro-BFD  Up        00:00:16  vlan1.120     NA
10.10.10.3/32
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
           Single Hop  ce11/1         1         4          Up

260      NA         IPv6       Micro-BFD  Up        00:00:09  vlan1.120     NA
fe80::e201:a6ff:fe4b:f301/128
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
           Single Hop  ce11/1         4         2052       Up


Number of Sessions:    4
```

R3

```
#show ipv6 pim neighbor

Total number of PIM neighbors:3

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::eac5:7aff:feb1:6b15                 xe8         00:02:55/00:01:22 1 / DR
fe80::36ef:b6ff:fe94:3db4                 vlan1.120   00:04:50/00:01:37 1 /
fe80::eac5:7aff:fea8:7cb9                 vlan1.120   00:04:51/00:01:27 1 / DR

#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
4100     NA         IPv4       Micro-BFD  Up        00:00:08  vlan1.120     NA
10.10.10.2/32
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
           Single Hop                  4         1          Up

4104     NA         IPv4       Micro-BFD  Up        00:00:08  vlan1.120     NA
10.10.10.1/32
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
         ============================================================
```

```
           Single Hop                 8         8          Up

4108      NA         IPv6       Micro-BFD   Up        00:00:07  vlan1.120     NA
fe80::36ef:b6ff:fe94:3db4/128
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
          ============================================================
           Single Hop                 2052      4          Up

4112      NA         IPv6       Micro-BFD   Up        00:00:07  vlan1.120     NA
fe80::eac5:7aff:fea8:7cb9/128
  HW SESS: TYPE        INTERFACE      LOC_DISC  REM_DISC   LOCAL_STATE
          ============================================================
           Single Hop                 2056      2052       Up


Number of Sessions:    4
```

R4

```
#show ipv6 pim neighbor

Total number of PIM neighbors:2

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::36ef:b6ff:fe94:3db4                 xe5         00:11:48/00:01:37 1 /
fe80::e201:a6ff:fe4b:f301                 xe5         00:08:51/00:01:24 1 /

#show ip pim neighbor

Total number of PIM neighbors:2

Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
10.10.10.2      xe5                00:09:03/00:01:25         v2    1 /
10.10.10.3      xe5                00:09:07/00:01:27         v2    1 / DR

#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
2056      2          IPv6       Single-Hop  Up        00:33:25  xe5          NA
fe80::36ef:b6ff:fe94:3db4/128
4         3          IPv4       Single-Hop  Up        00:22:04  xe5          NA
10.10.10.2/32

Number of Sessions:    2

#show ipv6 mld groups detail
MLD Connected Group Membership Details
```

```
Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      xe15
Group:          ff06::2
Flags:          R
Uptime:         00:01:18
Group mode:     Include ()
State:          Active
Last reporter:  fe80::1
Group source list: (R - Remote, M - SSM Mapping, S - Static )

Include Source List :
  Source Address                            Uptime    v2 Exp    Fwd  Flags
  5001::2                                   00:01:18  00:04:17  Yes  R

#show ip igmp groups detail
IGMP Instance wide G-Recs Count is: 1
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      xe15
Group:          231.1.1.1
Flags:          R
Uptime:         00:01:24
Group mode:     Include ()
State:          Active
Last reporter:  16.16.16.2
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Include Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  14.14.14.2      00:01:24  00:04:07  Yes  R
```

After Shutdown

```
#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr

Number of Sessions:    0
```

CHAPTER 5 PIM Source-Specific Multicast Configuration

Overview

PIM Source-Specific Multicast (SSM) is a multicast routing protocol that enhances the efficiency and security of multicast communication by enabling hosts to receive multicast traffic directly from specific sources. Here's a detailed overview of how PIM SSM operates using a subset of PIM sparse mode and IGMPv3/MLDv2:

SSM utilizes PIM sparse mode (PIM-SM) to create a Shortest Path Tree (SPT) directly between multicast sources and receivers. Hosts signal their interest using IGMPv3 (IPv4) or MLDv2 (IPv6), specifying the source IP address to join multicast groups without requiring a Rendezvous Point (RP). This direct communication approach optimizes multicast efficiency by bypassing the RP and establishing efficient data paths tailored to specific source-receiver relationships, enhancing network performance and security in multicast environments.

PIM Source-Specific Multicast (SSM) thus enhances multicast communication by streamlining the process of delivering multicast traffic directly from sources to receivers, leveraging existing multicast protocols and minimizing network complexity.

Feature Characteristics

PIM SSM enables hosts to specify source IP addresses when joining multicast groups, facilitating direct communication paths and eliminating the need for a Rendezvous Point (RP). It leverages PIM sparse mode to establish efficient Shortest Path Trees (SPTs) between sources and receivers, ensuring optimized multicast traffic delivery. Hosts use IGMPv3 (IPv4) and MLDv2 (IPv6) for precise membership management, enhancing network security and efficiency by reducing unnecessary traffic and simplifying configuration. SSM supports scalable deployment alongside existing multicast infrastructure, promoting interoperability and streamlined network administration while optimizing resource utilization and improving overall network reliability.

Benefits

The benefits of PIM SSM:

- Efficient Multicast Traffic Handling
- Optimized Resource Utilization
- Enhanced Security
- Simplified Configuration and Management
- Scalability and Compatibility
- Improved Network Performance
- Support for Diverse Applications.

PIM-SSM Configuration

The required steps to configure PIM-SSM 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 PIM-SSM on router.

All multicast group states are dynamically maintained as the result of IGMP Report/Leave and PIM Join/Prune messages.

Topology

The following figure displays the network topology used in these examples.

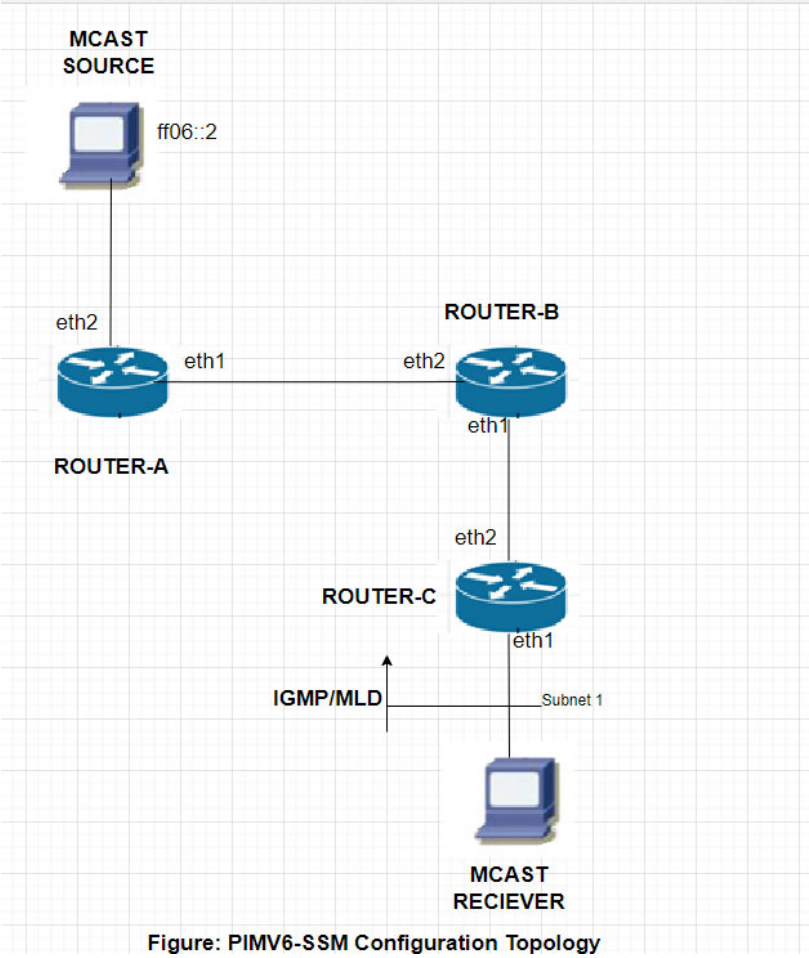


Figure: PIMV6-SSM Configuration Topology

Figure 5-1: PIM-SSM Configuration Topology

Configuration

Enable IP Multicast Routing on all Routers

Enable IP multicast routing on all of the PIM-SSM routers inside the PIM domain:

```
RouterA#configure terminal
RouterA(config)#ip multicast-routing
RouterA(config)#ipv6 multicast-routing
```

```
(config)#commit
```

Enable PIM SSM Default on all Routers

Enable PIM-SSM on all routers (Router_A, Router_B, and Router_C) inside the PIM domain on which you want to run PIM.

```
RouterA(config)# ip pim ssm default
RouterA(config)# ipv6 pim ssm default
RouterA(config)#commit
```

Enable PIM-SSM configuration on Router A

In the following sample configuration, both eth1 and eth2 are enabled for PIM-SSM on the router.

Enable PIM-SSM on all participating interfaces within router (Router_A) inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SSM on the router (Router_A).

```
RouterA(config)#interface eth1
RouterA(config-if)#ip address 10.1.1.1/24
RouterA(config-if)#ipv6 address 001::1/64
RouterA(config-if)#ip pim sparse-mode
RouterA(config-if)#ipv6 pim sparse-mode
RouterA(config-if)#ip igmp version 3
RouterA(config-if)#ipv6 mld version 2
RouterA(config-if)#commit
RouterA(config)#interface eth2
RouterA(config-if)#ip address 100.1.1.1/24
RouterA(config-if)#ipv6 address 2001::1/24
RouterA(config-if)#ip pim sparse-mode
RouterA(config-if)#ipv6 pim sparse-mode
RouterA(config-if)#ip igmp version 3
RouterA(config-if)#ipv6 mld version 2
RouterA(config-if)#commit
```

Enable PIM-SSM configuration on Router B

In the following sample configuration, both eth1 and eth2 are enabled for PIM-SSM on the router.

Enable PIM-SSM configuration on router B, configure Interface eth2 and eth1.

```
RouterB(config)#interface eth2
RouterB(config-if)#ip address 10.1.1.2/24
RouterB(config-if)#ipv6 address 3001::2/64
RouterB(config-if)#ip pim sparse-mode
RouterB(config-if)#ipv6 pim sparse-mode
RouterB(config-if)#ip igmp version 3
```

```
RouterB(config-if)#ipv6 mld version 2
RouterB(config-if)#commit
RouterB(config)#interface eth1
RouterB(config-if)#ip address 11.1.1.1/24
RouterB(config-if)#ipv6 address 4001::1/24
RouterB(config-if)#ip pim sparse-mode
RouterB(config-if)#ipv6 pim sparse-mode
RouterB(config-if)#ip igmp version 3
RouterB(config-if)#ipv6 mld version 2
RouterB(config-if)#commit
```

Enable PIM-SSM configuration on Router C

In the following sample configuration, both eth1 and eth2 are enabled for PIM-SSM on the router.

Enable PIM-SSM configuration on router C, configure Interface eth2 and eth1.

```
RouterC(config)#interface eth2
RouterC(config-if)#ip address 11.1.1.2/24
RouterC(config-if)#ipv6 address 4001::2/64
RouterC(config-if)#ip pim sparse-mode
RouterC(config-if)#ipv6 pim sparse-mode
RouterC(config-if)#ip igmp version 3
RouterC(config-if)#ipv6 mld version 2
RouterC(config-if)#exit
RouterC(config)#interface eth1
RouterC(config-if)#ip address 101.1.1.1/24
RouterC(config-if)#ipv6 address 5001::1/24
RouterC(config-if)#ip pim sparse-mode
RouterC(config-if)#ipv6 pim sparse-mode
RouterC(config-if)#ip igmp version 3
RouterC(config-if)#ipv6 mld version 2
RouterC(config-if)#commit
RouterC(config-if)#exit
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

Interface Details

The show ip pim interface command displays the interface details for Router_C, and shows that Router_C is the Designated Router on Subnet 1.

```
      Router_C#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

ROUTER C#show ipv6 pim interface
Total number of PIM interfaces:2
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Prior
eth2       0        v2/D   1      1
    Address       : fe80::eac5:7aff:fea8:7cb9
    Global Address: 3001::1
eth1      1        v2/D   0      1
    Address       : fe80::eac5:7aff:fea8:7cc3
    Global Address: 2001::1

ROUTER C#sh ipv6 pim neighbor

Total number of PIM neighbors:2

Neighbor Address                          Interface   Uptime/Expires    DR
                                                                        Pri/Mode
fe80::eac5:7aff:fea8:7cb9                 eth1        01:29:52/00:01:18  1 /
fe80::eac5:7aff:feb1:6b13                 eth2        01:29:49/00:01:28  1 /
```

Validation on IP Multicast Routing Table

Note: The multicast routing table displays for an S,G entries.

The show ip pim mroute command displays the IP multicast routing table. In this table, the following fields are defined:

```
LHR#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(101.1.1.2, 239.1.1.1)
RPF nbr: 10.1.1.2
RPF idx: xe14
SPT bit: 1
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o............................
```

```
(101.1.1.2, 239.1.1.1, rpt)
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..............................

LHR#sh ipv6 pim  mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(5001::2, ff06::2)
RPF nbr: fe80::36ef:b6ff:fe94:3ddd
RPF idx: xe14
SPT bit: 0
Upstream State: JOINED
 Local     ..i............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o............................

(5001::2, ff06::2, rpt)
RP: ::
RPF nbr: ::
RPF idx: None
Upstream State: RPT NOT JOINED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..............................
```

The ip igmp group detail and ipv6 mld group detail shows the source included (SSM)

```
LHR#show ip igmp groups
IGMP Instance wide G-Recs Count is: 1
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires   State    Last Reporte
r
239.1.1.1        xe26                 00:00:26   stopped   Active   100.1.1.2

LHR#show ip igmp groups detail
IGMP Instance wide G-Recs Count is: 1
```

```
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      xe26
Group:          239.1.1.1
Flags:          R
Uptime:         00:00:28
Group mode:     Include ()
State:          Active
Last reporter:  100.1.1.2
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Include Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  101.1.1.2       00:00:28  00:03:56  Yes  R

LHR#show ipv6 mld groups
MLD Connected Group Membership
Group Address                           Interface            Uptime   Expires  S
tate    Last Reporter
ff06::2                                 xe26                 00:00:31  stopped A
ctive   fe80::1

LHR#show ipv6 mld groups detail
MLD Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      xe26
Group:          ff06::2
Flags:          R
Uptime:         00:00:32
Group mode:     Include ()
State:          Active
Last reporter:  fe80::1
Group source list: (R - Remote, M - SSM Mapping, S - Static )

Include Source List :
  Source Address                        Uptime    v2 Exp    Fwd  Flags
  5001::2                               00:00:32  00:03:49  Yes  R
```

CHAPTER 6 Bidirectional-PIM Configuration

Bidirectional PIM (BIDIR-PIM) is a variant of PIM Sparse-Mode (PIM-SM) that builds bidirectional shared trees connecting multicast sources and receivers as specified in RFC5015.

BIDIR-PIM dispenses with both encapsulation and source state by allowing packets to be natively forwarded from a source to the Rendezvous Point (RP) using shared tree state.

BIDIR-PIM uses the same tree for traffic from source towards RP and from RP to receivers.

Note: Multicast PIM BIDIR feature is not supported in Qumaran 2 (Q2) and J2C+ platform.

Designated Forwarders (DF) Election

Bidirectional Shared-Trees violates current (*, G) RPF rules, as it accepts traffic from one Reverse Path Forwarding (RPF) interface only. To avoid forwarding multicast packet looping, bidir-PIM introduces a new mechanism called the designated forwarder (DF) election.

The designated forwarder (DF) election takes place for all PIM routers on every network segment and point-to-point link. The procedure selects one router as the DF for every RP of bidirectional groups. The designated forwarder is responsible for forwarding multicast packets received on that network.

PIM-SM Configuration

Enabling BIDIR-PIM

`#configure terminal`	Enter Configure mode.
`(config)#ip pim bidir-enable`	Enable bidir-pim
`(config)#commit`	Commit the transaction.

Configuring BIDIR Rendezvous Point Statically

Configuring Static BIDIR RP

`#configure terminal`	Enter configure mode.
`(config)#ip access-list standard ip1` `(config-ip-acl-std)#permit 224.0.0.0/24`	Configure the access list for multicast group.
`(config)#ip pim rp-address 10.10.1.5 ip1 bidir`	Statically configure an rp address for multicast groups.
`(config)#commit`	Commit the transaction.

Here is the sample configuration for `Router_D`:

```
hostname Router_D
!
       ip access-list standard ip1
        permit 224.0.0.0/24
      !
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
      ip multicast bidirectional enable
!
ip pim bidir-enable
ip pim rp-address 10.10.1.5 ip1 bidir
!
```

Validation

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `22.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5 bidir
         Uptime: 00:01:45
```

At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.5.37
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1.`

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr`	Displays the unicast next-hop to reach RP.
	and mask length.
`RPF idx`	Displays the incoming interface for this (*, G) state.
`RP`	Displays the IP address for the RP router
`B`	Displays the bidirectional pim mode
`The leading dots ....`	Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
 Local     ..............................
 Joined    j..............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and the RP is reachable through `eth2`. The ‘B’ flag indicates that it is in bidirectional pim mode.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
 Local     ..............................
 Joined    j..............................
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface (TTL)

(*, 224.0.1.3), uptime 00:00:07, stat expires 00:03:23
Owner PIM, Flags: TFB
  Outgoing interface list:
    eth2 (1)
    eth1 (1)
```

Configuring BIDIR-Neighbor Filter

This section shows how to configure a bidir-neighbor filter to specify which bidirectionally capable (bidir-capable) neighbors will participate in the designated forwarder (DF) election.

`#configure terminal`	Enter configure mode
`(config)# interface eth1`	Enter interface mode
`(config-if)# ip pim bidir-neighbor-filter Acl-name/acl-no`	Configure bidir-neighbor-filter at interface
`(config-if)# no ip pim bidir-neighbor-filter acl-name/acl-no`	Unconfigure bidir-neighbor-filter at interface

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
rtr6#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
192.168.1.149   eth1               00:00:44/00:01:31         v2    1 / B
192.168.1.152   eth1               00:00:01/00:01:44         v2    1 / DR  ------
--?B Flag is removed

rtr6#show running-config interface eth1
!
interface eth1
 ip address 192.168.1.57/24
 no shutdown
 no snmp trap link-status
 ip ospf cost 10
 ip pim bidir-neighbor-filter 1
 ip pim sparse-mode
 lldp-agent
 no dcbx enable
 exit
```

Configuring BIDIR PIM Offer Message Interval Time

This section shows how to configure BIDIR PIM offer message interval time.

`#configure terminal`	Enter configure mode.

`(config)# ip pim bidir-offer-interval <1>`	Specify offer-interval in the range 1-20000
`(config-if)# no ip pim bidir-offer-interval`	Disable offer-interval

Validation

1. Verify the time set for offer message interval

```
(config)#ip pim  bidir-offer-interval 10

#show  running-config
!
no service password-encryption
!
debug nsm packet
debug ip pim events
debug ip pim mfc
debug ip pim packet
debug ip pim state
debug ip pim timer
debug ip pim mib
!
ip vrf management
!
mpls propagate-ttl
!
no ip icmp-broadcast
!
ip multicast-routing
ip multicast bidirectional enable
!
ip pim bidir-enable
ip pim bidir-offer-interval 10
ip pim rp-address 172.31.5.153 bi
```

2. Verify neighbor information in Bidirectional PIM mode with “B” flag associated

```
rtr6#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
192.168.1.149   eth1               00:38:36/00:01:39         v2    1 / B
192.168.1.152   eth1               00:37:53/00:01:22         v2    1 / DR B
rtr6#
```

3. Verify DF status per interface

```
rtr6#show ip pim interface df
Interface RP               DF Winner        Metric
eth1      172.31.5.153     192.168.1.152    20
eth2      172.31.5.153     192.168.10.57    30
rtr6#
rtr6#show ip pim interface eth1 df 172.31.5.153

 Designated Forwarder election for eth1, 192.168.1.57, RP 172.31.5.153
 State                          Non-DF (Lose)
```

```
 Offer count is                  0
 Current DF ip address           192.168.1.152
 Last winner metric preference   110
 Last winner metric              20
rtr6#
```

Configuring BIDIR PIM Offer Interval Limit

This section shows how to configure the Protocol Independent Multicast (PIM) bidirectionally capable number of unanswered offers before it changes as the designated forwarder (DF).

`#configure terminal`	Enter Configure mode.
`(config)# ip pim bidir-offer-limit <offer packet limit>`	Configure bidir-offer-limit
`(config-if)# no ip pim bidir-offer-limit`	Disable offer-limit

Validation

```
rtr6#show  running-config
!
no service password-encryption
!
hostname rtr6
!
!
debug nsm packet
!
ip vrf management
!
mpls propagate-ttl
!
no ip icmp-broadcast
!
access-list 1 deny 192.168.1.152
access-list 1 permit any

!
ip multicast-routing
!
ip pim bidir-enable
ip pim bidir-offer-limit 5
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
```

CHAPTER 7 MSDP Configuration

Multicast Source Discovery Protocol (MSDP) is used to exchange multicast source information between BGP-enabled PIM-SM domains. Using MSDP, routers in a PIM-SM domain can rely on their own RP to reach a source in a different PIM-SM domain.

Overview

MSDP routers in a PIM-SM domain have a MSDP peering relationship with MSDP peers in another domain using a TCP connection. MSDP peering is the first step towards exchanging inter-domain multicast source information using MSDP SA (Source-Active) messages.

When an RP in a PIM-SM domain first learns of a new sender (via PIM register messages), it constructs an SA message and sends it to its MSDP peers.

All RPs which intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer.

An SA message contains these fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Each SA message received from a MSDP peer goes through an RPF check. The peer-RPF check compares the RP address carried in the SA message with the MSDP peer from which the message was received:

- If the MSDP peer receives an SA from a non-RPF peer towards the originating RP, it drops the message.
- Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an RP receives a new SA message from a peer in another domain, it checks if there are any receivers interested in the traffic. An RP checks for a (*, G) entry with a non-empty outgoing list. If the outgoing list is non-empty, the RP sends a (S,G) join towards the source.

Caching SA state

If a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to learn about the source. MSDP SA caching is done at MSDP peers to reduce join latency for new receivers. The SA cache is populated as soon an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

MSDP Mesh groups are used inside a PIM-SM domain to ease RPF checking and SA forwarding within the domain. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. This reduces SA message flooding and simplifies peer-RPF flooding.

© 2026 IP Infusion Inc. Proprietary

MSDP Default Peer

An MSDP default peer is used when MSDP peers are not BGP peers. SA messages coming from a default peer do not go through an RPF check and are always accepted.

Configure PIM-SM

For the MSDP topology in Figure 7-11, you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see Chapter 1, *PIM Sparse Mode*.

Configure MSDP

In the topology in Figure 7-11, an MSDP session is established between RTR-1 and RTR-2 in both domains. The following sample configuration on RTR-1 shows how to enable MSDP peering between RTR-1 and RTR-2.

Topology

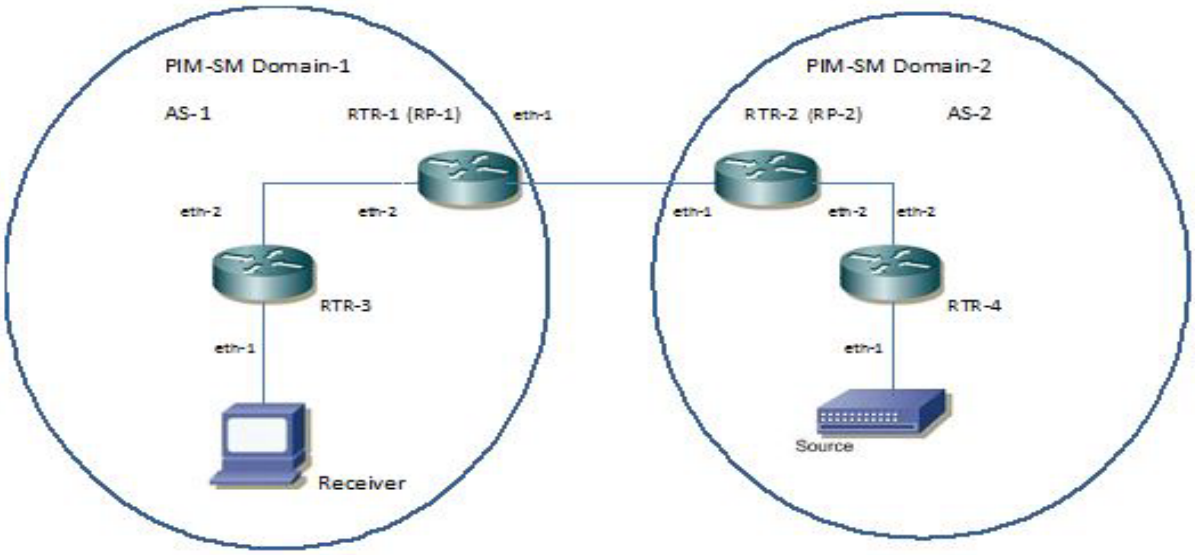


Figure 7-1: MSDP topology

IP addresses:

RTR-1 eth1: 11.1.1.11

RTR-1 eth2: 10.1.1.11

RTR-2 eth1: 11.1.1.12

RTR-2 eth2: 12.1.1.12

RTR-4 eth1: 12.1.1.14

RTR-4 eth2: 20.1.1.14

RTR-3 eth1: 13.1.1.13

RTR-3 eth2: 10.1.1.13

Source: 20.1.1.10

Multicast group: 224.1.1.1

RTR-1

`#configure terminal`	Enter configure mode.

`(config)#ip msdp peer 11.1.1.12`
--or--
`(config)#ip msdp peer 11.1.1.12 connect source eth1`
	Configure a MSDP peer.
	
	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.

`(config)#ip msdp password myPass peer 11.1.1.12`	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
`(config)#ip msdp default-peer 11.1.1.12`	Configure MSDP default peer.
`(config)#ip msdp mesh-group mesh1 11.1.1.12`	Configure MSDP mesh group.
`(config)#ip msdp originator-id eth2`	Configure MSDP originator identifier.
`(config)#commit`	Commit the transaction.

Validation

RTR-1

```
#show running-config

ip msdp peer 11.1.1.12
ip msdp default-peer 11.1.1.12
ip msdp mesh-group mesh1 11.1.1.12
ip msdp password myPass peer 11.1.1.12
ip msdp originator-id eth2
ip multicast-routing
!
ip pim register-rp-reachability
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
ip pim vrf management register-rp-reachability
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.175/24
 no shutdown
!
```

```
interface eth1
 ip address 11.1.1.11/24
no shutdown
 ip pim sparse-mode
ip pim bsr-border
!
interface eth2
 ip address 10.1.1.11/24
 no shutdown
ip pim sparse-mode
!
interface eth3
 no shutdown
!
interface pimreg
 no multicast
 no shutdown
!
router ospf 100
 network 10.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 1
neighbor 11.1.1.12 remote-as 2
!
line con 0
 login
line vty 0 39
 login
!
```

This command shows the MSDP peer information at RTR-1:

```
#show ip msdp peer
MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

In the MSDP topology in Figure 7-11, when a source sends multicast traffic for group 224.1.1.1, RTR-4 (the DR) sends a register packet towards RTR-2 which is the RP in the domain. RTR-2 receives the register packet and sends an MSDP SA message to its MSDP peer (RTR-1). RTR-1 receives the SA message and creates an entry in the SA cache containing the source, group, and RP information.

This command at RTR-1 shows the SA information with source address, group address, and RP address:

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02 Exptime
00:03:28P
```

RTR-3 receives an IGMP join for group 224.1.1.1 and joins the shared tree path toward the RP (RTR-1).

When RTR-1 receives an SA message from RTR-2, because it has a receiver, it sends an (S,G) join towards the source. Now traffic from the source is received at RTR-1 via the shortest path tree formed between RTR-1 and the source. RTR-1 distributes traffic downstream towards the receiver.

This command shows the PIM state at RTR-1 upon receiving an SA message and joining towards the source:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 224.1.1.1)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 11.1.1.12
RPF idx: eth1
SPT bit: 0
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o.............................

(20.1.1.10, 224.0.1.3, rpt)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ................................
 Pruned    ................................
 Outgoing  ..o.............................
```

RTR-2

This command shows the MSDP peer information at RTR-2.

```
#show  ip msdp  peer
MSDP Peer 11.1.1.11
Connection status
 State: Up (Established)
 Keepalive sent: 2
```

```
Keepalive received: 2
```

CHAPTER 8 VRRP Aware PIM Configuration

VRRP Aware PIM is a redundancy mechanism for the Protocol Independent Multicast to interoperate with the Virtual Router Redundancy Protocol. It helps PIM to track VRRP state changes and to preserve multicast traffic upon failover. In order to ensure that the PIM DR is always able to forward PIM Join/Prune message towards RP, the VRRP master router becomes the PIM DR.

Topology

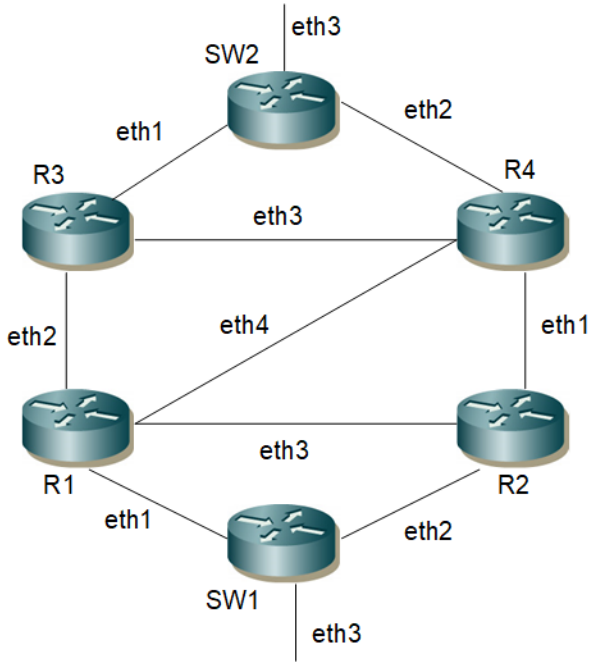


Figure 8-1: VRRP Aware PIM Topology

In the configs below IGMP host is towards SW1 and source is towards SW2.

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`SW1(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`SW1(config)#interface eth1`	Enter interface mode.
`SW1(config-if)#switchport`	Configure eth1 as a layer 2 port.
`SW1(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW1(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW1(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`SW1(config-if)#exit`	Exit interface mode.
`SW1(config)#interface eth2`	Enter interface mode.

SW1(config-if)#switchport	Configure eth2 as a layer 2 port.
SW1(config-if)#bridge-group 1	Associate bridge to an interface.
SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth2 interface.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth3	Enter interface mode.
SW1(config-if)#switchport	Configure eth3 as a layer 2 port.
SW1(config-if)#bridge-group 1	Associate bridge to an interface.
SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#no igmp snooping	Disable IGMP snooping
SW1(config)#commit	Commit the transaction.

R1

R1#configure terminal	Enter configure mode.
R1(config)#bridge 1 protocol ieee vlan-bridge	Configure bridge as IEEE VLAN bridge
R1(config)#vlan 2 bridge 1 state enable	Configure VLANs
R1(config)#ip multicast-routing	Configure multicast routing on R1
R1(config)#ip pim rp-address 1.1.1.4	Statically configure RP address for multicast groups.
R1(config)#interface lo	Enter interface mode.
R1(config-if)#ip address 1.1.1.1/32	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#exit	Exit interface mode.
R1(config)#interface eth1	Enter interface mode.
R1(config-if)#switchport	Configure eth3 as a Layer 2 port.
R1(config-if)#bridge-group 1	Associate bridge to an interface.
R1(config-if)#switchport mode trunk	Configure port as a trunk.
R1(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface vlan1.2	Enter interface mode.
R1(config-if)#ip address 100.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
R1(config-if)#ip pim redundancy 1 vrrp dr-priority 101	Configure VRRP aware PIM command with dr-priority and VRRP instance
R1(config)#interface eth2	Enter interface mode.
R1(config-if)#ip address 20.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#ip pim sparse-mode	Configure PIM as sparse mode

`R1(config)#interface eth3`	Enter interface mode.
`R1(config-if)#ip address 29.1.1.1/24`	Configure the IP address of the interface.
`R1(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface eth4`	Enter interface mode.
`R1(config-if)#ip address 5.1.1.1/24`	Configure the IP address of the interface.
`R1(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#router ospf 1`	Set the routing process ID.
`R1(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Configure OSPF network in area 0
`R1(config-router)#ospf router-id 1.1.1.1`	Configure OSPF router-ID
`R1(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R1(config-router)#network 29.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R1(config-router)#network 5.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R1(config-router)#exit`	Exit router mode.
`R1(config)#router vrrp 1 vlan1.2`	Create a VRRP instance for interface VLAN1.2
`R1(config-router)#virtual-ip 100.1.1.1`	Set the virtual IP address for the VRRP session
`R1(config-router)#enable`	Enable the VRRP session on the router.
`R1(config-router)#commit`	Commit the transaction.

R2

`R2#configure terminal`	Enter configure mode.
`R2(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`R2(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`R2(config)#ip multicast-routing`	Configure multicast routing on R2
`R2(config)#ip pim rp-address 1.1.1.4`	Statically configure RP address for multicast groups.
`R2(config)#interface lo`	Enter interface mode.
`R2(config-if)#ip address 1.1.1.2/32`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface eth1`	Enter interface mode.
`R2(config-if)#ip address 50.1.1.2/24`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config)#interface eth2`	Enter interface mode.
`R2(config-if)#switchport`	Configure eth3 as a Layer 2 port.
`R2(config-if)#bridge-group 1`	Associate bridge to an interface.
`R2(config-if)#switchport mode trunk`	Configure port as a trunk.

`R2(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`R2(config)#interface eth3`	Enter interface mode.
`R2(config-if)#ip address 29.1.1.2/24`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface vlan1.2`	Enter interface mode.
`R2(config-if)#ip address 100.1.1.2/24`	Configure the IP address of the interface.
`R2(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R2(config-if)#ip pim redundancy 1 vrrp dr-priority 101`	Configure VRRP aware PIM command with dr-priority and VRRP instance
`R2(config)#router ospf 1`	Set the routing process ID .
`R2(config-router)#ospf router-id 1.1.1.2`	Configure OSPF router-ID
`R2(config-router)#network 1.1.1.2/32 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#network 29.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#network 50.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R2(config-router)#exit`	Exit router mode.
`R2(config)#router vrrp 1 vlan1.2`	Create a VRRP instance for interface VLAN1.2
`R2(config-router)#virtual-ip 100.1.1.1`	Set the virtual IP address for the VRRP session
`R2(config-router)#enable`	Enable the VRRP session on the router.
`R2(config-router)#commit`	Commit the transaction.

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`R3(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`R3(config)#ip multicast-routing`	Configure multicast routing on R3
`R3(config)#ip pim rp-address 1.1.1.4`	Statically configure RP address for multicast groups.
`R3(config)#interface lo`	Enter interface mode.
`R3(config-if)#ip address 1.1.1.3/32`	Configure the IP address of the interface.
`R3(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface eth1`	Enter interface mode.
`R3(config-if)#switchport`	Configure eth3 as a Layer 2 port.
`R3(config-if)#bridge-group 1`	Associate bridge to an interface.
`R3(config-if)#switchport mode trunk`	Configure port as a trunk.
`R3(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`R3(config)#interface eth2`	Enter interface mode.

`R3(config-if)#ip address 20.1.1.2/24`	Configure the IP address of the interface.
`R3(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R3(config)#interface eth3`	Enter interface mode.
`R3(config-if)#ip address 45.1.1.2/24`	Configure the IP address of the interface.
`R3(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface vlan1.2`	Enter interface mode.
`R3(config-if)#ip address 200.1.1.2/24`	Configure the IP address of the interface.
`R3(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#router ospf 1`	Set the routing process ID.
`R3(config-router)#ospf router-id 1.1.1.3`	Configuring OSPF router-ID.
`R3(config-router)#network 1.1.1.3/32 area 0.0.0.0`	Configure OSPF network in area 0.
`R3(config-router)#network 200.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0.
`R3(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0.
`R3(config-router)#network 45.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0.
`R3(config-router)#commit`	Commit the transaction.

R4

`R4#configure terminal`	Enter configure mode.
`R4(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`R4(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`R4(config)#ip multicast-routing`	Configure multicast routing on R4
`R4(config)#ip pim rp-address 1.1.1.4`	statically configure RP address for multicast groups.
`R4(config)#interface lo`	Enter interface mode.
`R4(config-if)#ip address 1.1.1.4/32`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface eth1`	Enter interface mode.
`R4(config-if)#ip address 50.1.1.1/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config)#interface eth2`	Enter interface mode.
`R4(config-if)#switchport`	Configure eth3 as a Layer 2 port.
`R4(config-if)#bridge-group 1`	Associate bridge to an interface.
`R4(config-if)#switchport mode trunk`	Configure port as a trunk.
`R4(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.

`R4(config)#interface eth3`	Enter interface mode.
`R4(config-if)#ip address 45.1.1.1/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface eth4`	Enter interface mode.
`R4(config-if)#ip address 5.1.1.2/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface vlan1.2`	Enter interface mode.
`R4(config-if)#ip address 200.1.1.1/24`	Configure the IP address of the interface.
`R4(config-if)#ip pim sparse-mode`	Configure PIM as sparse mode
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#router ospf 1`	Set the routing process ID .
`R4(config-router)#ospf router-id 1.1.1.4`	Configuring OSPF router-ID
`R4(config-router)#network 1.1.1.4/32 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 200.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 45.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 50.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#network 5.1.1.0/24 area 0.0.0.0`	Configure OSPF network in area 0
`R4(config-router)#commit`	Commit the transaction.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge as IEEE VLAN bridge
`SW2(config)#vlan 2 bridge 1 state enable`	Configure VLANs
`SW2(config)#interface eth1`	Enter interface mode.
`SW2(config-if)#switchport`	Configure eth1 as a Layer 2 port.
`SW2(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW2(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW2(config-if)#switchport trunk allowed vlan add 2`	Allow VLAN 2 on the eth1 interface.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface eth2`	Enter interface mode.
`SW2(config-if)#switchport`	Configure eth2 as a Layer 2 port.
`SW2(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW2(config-if)#switchport mode trunk`	Configure port as a trunk.

© 2026 IP Infusion Inc. Proprietary

SW2(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth2 interface.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth3	Enter interface mode.
SW2(config-if)#switchport	Configure eth3 as a Layer 2 port.
SW2(config-if)#bridge-group 1	Associate bridge to an interface.
SW2(config-if)#switchport mode trunk	Configure port as a trunk.
SW2(config-if)#switchport trunk allowed vlan add 2	Allow VLAN 2 on the eth1 interface.
SW2(config-if)#commit	Commit the transaction.

Validation

Verify that PIM DR is the same node as VRRP Master.

Validation 1

```
R1#show  ip ospf  neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface            Instance ID
1.1.1.5           1   Full/DR         00:00:31    5.1.1.2         eth4                   0
1.1.1.3           1   Full/DR         00:00:36    10.2.3.2        eth3                  0
1.1.1.4           1   Full/DR         00:00:35    10.2.4.2        eth2                  0

R1#show  vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Master
 Virtual IP address: 100.1.1.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 100.1.1.1
 Operational master IP address: 100.1.1.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Master uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE

R1#show  ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
```

```
5.1.1.2         eth4                 01:55:57/00:01:18         v2    1 / DR
10.2.4.2        eth2                01:45:57/00:01:18         v2    1 / DR
10.2.3.2        eth3                02:13:01/00:01:44         v2    1 / DR
100.1.1.2       vlan1.2             00:01:39/00:01:29         v2    1 /

R1#show  ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 5
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1

(*, 224.1.1.1)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    .............................
 Asserted  .............................
FCR:
Source: 200.1.1.5
 Outgoing  .....o.........................
 KAT timer running, 116 seconds remaining
 Packet count 1

(*, 224.1.1.2)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    .............................
 Asserted  .............................
FCR:

(*, 224.1.1.3)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    .............................
 Asserted  .............................
FCR:

(*, 224.1.1.4)
```

```
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:

(*, 224.1.1.5)
RP: 1.1.1.4
RPF nbr: 5.1.1.2
RPF idx: eth4
Upstream State: JOINED
 Local     .....i.........................
 Joined    ..............................
 Asserted  ..............................
FCR:

R1#show  ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(200.1.1.5, 224.1.1.1), uptime 00:01:38, stat expires 00:02:43
Owner PIM, Flags: TF
  Incoming interface: eth4
  Outgoing interface list:
    vlan1.2 (1)
```

Validation 2

```
R2#show  ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                           Priority/Mode
10.2.3.1        eth3                02:13:36/00:01:31         v2    1 /
10.3.5.2        eth1                00:07:45/00:01:30         v2    1 / DR
100.1.1.1       vlan1.2            00:02:14/00:01:36         v2    101 / DR

R2#show  ip pim neighbor detail
Nbr 10.2.3.1 (eth3)
 Expires in 87 seconds, uptime 02:13:40
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 1, Gen ID: 234024133,
 Interface ID: Router-ID: 1.1.1.2 Local-ID: 10030,

Nbr 10.3.5.2 (eth1), DR
 Expires in 86 seconds, uptime 00:07:49
```

```
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 1, Gen ID: 2078598240,
 Interface ID: Router-ID: 1.1.1.5 Local-ID: 10050,

Nbr 100.1.1.1 (vlan1.2), DR
 Expires in 91 seconds, uptime 00:02:18
 Holdtime: 105 secs, T-bit: off, Lan delay: 500, Override interval: 2500
 DR priority: 101, Gen ID: 379671611,
 Interface ID: Router-ID: 1.1.1.2 Local-ID: 10066,

R2#show  vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1.2
 State: AdminUp   - Backup
 Virtual IP address: 100.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 100.1.1.2
 Operational master IP address: 100.1.1.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 1 hours 30 minutes 5 seconds (540500 centi sec)
 Skew time: 60 centi sec
 Master Down Interval: 360 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.2: JOINED
 V2-Compatible: FALSE
```

Protocol Independent Multicasting Command Reference

CHAPTER 1 PIMv4 Commands

The chapter includes the commands that support the Protocol-Independent Multicast (PIM).

- clear ip mroute
- clear ip msdp peer
- clear ip msdp sa-cache
- clear ip pim sparse-mode
- debug ip pim
- debug ip pim packet
- debug pim bfd
- debug ip pim timer assert
- debug ip pim timer bsr
- debug ip pim timer hello
- debug ip pim timer joinprune
- debug ip pim timer register
- ip msdp default-peer
- ip msdp mesh-group
- ip msdp originator-id
- ip msdp password
- ip msdp peer
- ip msdp sa
- ip pim
- p pim accept-register
- ip pim anycast-rp
- ip pim bfd
- ip pim bfd all-interfaces
- ip pim bidir-enable
- ip pim bidir-offer-interval
- ip pim bidir-offer-limit
- ip pim bidir-neighbor-filter
- ip pim bind ecmp-bundle
- ip pim bsr-border
- ip pim bsr-candidate
- ip pim crp-cisco-prefix
- ip pim dr-priority
- ip pim ecmp-bundle
- ip pim exclude-genid
- ip pim hello-holdtime

© 2026 IP Infusion Inc. Proprietary

- ip pim hello-interval
- ip pim ignore-rp-set-priority
- ip pim jp-timer
- ip pim neighbor-filter
- ip pim passive
- ip pim propagation-delay
- ip pim redundancy
- ip pim register-rate-limit
- ip pim register-rp-reachability
- ip pim register-source
- ip pim register-suppression
- ip pim router-id
- ip pim rp-address
- ip pim rp-candidate
- ip pim rp-register-kat
- ip pim spt-threshold
- ip pim ssm
- ip pim state-refresh origination-interval
- ip pim unicast-bsm
- show debugging ip pim
- show debugging pim
- show ip msdp peer
- show ip msdp sa-cache
- show ip pim ecmp-bundle
- show ip pim interface
- show ip pim interface df
- show ip pim mroute
- show ip pim neighbor
- show ip pim nexthop
- show ip pim bsr-router
- show ip pim local-members
- show ip pim rp-hash
- show ip pim rp mapping
- snmp restart pim

© 2026 IP Infusion Inc. Proprietary

clear ip mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax

```
clear ip mroute *
clear ip mroute * pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D
clear ip mroute A.B.C.D A.B.C.D
clear ip mroute A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D pim sparse-mode
clear ip mroute statistics *
clear ip mroute statistics A.B.C.D
clear ip mroute statistics A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) *
clear ip mroute (vrf NAME|) * pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D pim sparse-mode
clear ip mroute (vrf NAME|) statistics *
clear ip mroute (vrf NAME|) statistics A.B.C.D
clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`*`	Delete all multicast routes
`pim`	Protocol Independent Multicast (PIM)
`A.B.C.D`	Clears group IP address
`A.B.C.D`	Clears source IP address
`dense-mode`	Clears multicast rout table for PIM dense-mode
`sparse-mode`	Clears multicast route table for PIM sparse mode
`statistics`	Clears multicast route statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip mroute * pim sparse-mode
#clear ip mroute 224.2.2.2 4.4.4.4 pim sparse-mode
```

clear ip msdp peer

Use this command to clear the TCP connection to a Multicast Source Discovery Protocol (MSDP) peer.

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Command Syntax

```
clear ip msdp peer (A.B.C.D|)
clear ip msdp (vrf NAME|) peer (A.B.C.D|)
```

Parameters

A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#clear ip msdp peer 192.168.1.26
```

clear ip msdp sa-cache

Use this command to clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries.

Command Syntax

```
clear ip msdp sa-cache (A.B.C.D |)
clear ip msdp (vrf NAME|) sa-cache (A.B.C.D |)
```

Parameters

A.B.C.D	Multicast group address; if not specified, all SA cache entries are cleared
NAME	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#clear ip msdp sa-cache 225.25.25.1
```

clear ip pim sparse-mode

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax

```
clear ip pim sparse-mode bsr rp-set *
clear ip pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rp-set`	PIMv2 bootstrap router RP set
`bsr`	PIMv2 Bootstrap Router
`*`	Clear all RP sets

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip pim sparse-mode bsr rp-set *
```

debug ip pim

Use this command to enable debugging for PIM.

Use the `no` option with this command to deactivate debugging for PIM.

Command Syntax

```
debug ip pim (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
debug ip pim (vrf
  NAME|)(all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
no debug ip pim (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
no debug ip pim (vrf NAME|) (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet
  |state|timer)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`all`	Enable debugging for all PIM events
`events`	Enable debugging for general configuration, VRF context
`mfc`	Enable debugging for MFC updates
`mib`	Enable debugging for MIB entries
`mtrace`	Enable debugging for MTRACE messages
`msdp`	Enable debugging for MSDP
`nexthop`	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
`nsm`	Enable debugging for NSM
`packet`	Enable debugging for PIM packets
`state`	Enable debugging for PIM states
`timer`	Enable debugging for PIM timers

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ip pim all
```

debug ip pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the `no` option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax

```
debug ip pim packet
debug ip pim packet in
debug ip pim packet out
debug ip pim (vrf NAME|) packet
debug ip pim (vrf NAME|) packet in
debug ip pim (vrf NAME|) packet out
no debug ip pim packet
no debug ip pim packet in
no debug ip pim packet out
no debug ip pim (vrf NAME|) packet
no debug ip pim (vrf NAME|) packet in
no debug ip pim (vrf NAME|) packet out
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`in`	Debug incoming packets
`out`	Debug outgoing packets

Default

By default, all debug options are disabled.

Command Mode

Configure and Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip pim packet in
```

debug pim bfd

Use this command to print all the PIM BFD session related logs, this command is for all VRF instances and address families (PIMv4 and PIMv6).

Use the `no` option to disable PIM BFD logging.

Command Syntax

```
debug pim bfd

no debug pim bfd
```

Parameters

None

Default

By default, PIM BFD logging is disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
# terminal
(config)#debug pim bfd
```

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 (vrf NAME|) timer assert
no debug ip pim timer assert
no debug ip pim (vrf NAME|) timer assert
```

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 and updated in OcNOS version 6.2.0.

Example

```
#debug ip pim timer assert
```

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 (vrf NAME|) timer register
no debug ip pim timer register
no debug ip pim (vrf NAME|) timer register
```

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 ip pim timer register
```

ip msdp default-peer

Use this command to set a Multicast Source Discovery Protocol (MSDP) peer from which to accept Source-Active (SA) messages.

You can have multiple active default peers:

- When you enter multiple `ip msdp default-peer` commands *with* a `prefix-list` keyword, all the default peers are used at the same time for different RP prefixes. This form is typically used in a service provider cloud that connects stub site clouds.
- When you enter multiple `ip msdp default-peer` commands *without* a `prefix-list` keyword, a single active peer accepts all SA messages. If that peer fails, the next configured default peer accepts all SA messages. This form is typically used at a stub site.

Use the `no` option with this command to stop accepting SA messages from a peer.

Command Syntax

```
ip msdp default-peer A.B.C.D (prefix-list WORD|)
ip msdp (vrf NAME|) default-peer A.B.C.D (prefix-list WORD|)
no ip msdp default-peer A.B.C.D
no ip msdp (vrf NAME|) default-peer A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address of a previously configured MSDP peer
`prefix-list`	Make this the default peer only for an access list of rendezvous points (RPs):
`WORD`	Access list name
`NAME`	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp default-peer 192.168.1.26 prefix-list xyz
```

ip msdp mesh-group

Use this command to add a Multicast Source Discovery Protocol (MSDP) peer to a mesh group.

You can set up multiple mesh groups on the same device and multiple peers per mesh group.

Use the `no` option with this command to remove a peer from a mesh group.

Command Syntax

```
ip msdp mesh-group WORD A.B.C.D
ip msdp (vrf NAME|) mesh-group WORD A.B.C.D
no ip msdp mesh-group WORD A.B.C.D
no ip msdp (vrf NAME|) mesh-group WORD A.B.C.D
```

Parameters

`WORD`	Name of the mesh group
`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp mesh-group mg-1 192.168.1.26
```

ip msdp originator-id

Use this command to allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of an interface as a rendezvous point (RP) address in the SA message.

By default, OcNOS uses the RP address of the device.

Use the `no` option with this command to use the RP address of the device in SA messages.

Command Syntax

```
ip msdp originator-id IFNAME
ip msdp (vrf NAME|) originator-id IFNAME
no ip msdp originator-id IFNAME
no ip msdp (vrf NAME|) originator-id IFNAME
```

Parameters

`IFNAME`	Use the IP address of this interface as an RP address in SA messages
`NAME`	Name of the VPN routing/forwarding instance

Default

The RP address is used as the originator ID.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp originator-id eth2
```

ip msdp password

Use this command to set an MD5-shared password key used for authenticating a Multicast Source Discovery Protocol (MSDP) peer. By default, no MD5 password is enabled.

Use the `no` option with this command to remove a password.

Command Syntax

```
ip msdp password WORD peer A.B.C.D
ip msdp (vrf NAME|) password WORD peer A.B.C.D
no ip msdp password WORD peer A.B.C.D
no ip msdp (vrf NAME|) password WORD peer A.B.C.D
```

Parameters

`WORD`	Password
`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Default

The MD5 password authentication for TCP connections between MSDP peer is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp password S#m*u104!! peer 192.168.1.26
```

ip msdp peer

Use this command to configure an Multicast Source Discovery Protocol (MSDP) peer relationship.

Use the `no` option with this command to remove a peer relationship.

Command Syntax

```
ip msdp peer A.B.C.D ((connect-source (IFNAME))|)
ip msdp (vrf NAME|) peer A.B.C.D ((connect-source (IFNAME))|)
ip msdp peer A.B.C.D connect-source A.B.C.D
ip msdp (vrf Name|) peer A.B.C.D connect-source A.B.C.D
no ip msdp peer A.B.C.D
no ip msdp (vrf NAME|) peer A.B.C.D
```

Parameters

`A.B.C.D`	IP address of the potential peer
`A.B.C.D`	IP address of local peer
`IFNAME`	Use the primary address of this interface for the TCP connection with the peer
`NAME`	Name of the VPN routing/forwarding instance

Default

By default, all ip msdp options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp peer 192.168.1.26 connect-source eth2
```

ip msdp sa

Use this command to configure an msdp source active entry.

Use the `no` form of this command to remove an msdp source active entry configuration.

Command Syntax

```
ip msdp (vrf NAME|) sa s A.B.C.D g A.B.C.D r A.B.C.D
no ip msdp (vrf NAME|) sa s A.B.C.D g A.B.C.D
```

Parameters

`NAME`	Name of the VPN routing/forwarding instance name
`A.B.C.D`	IP address of the remote peer
`A.B.C.D`	IP address of the remote group
`A.B.C.D`	IP address of the remote RP

Default

By default, all ip msdp options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip msdp sa s 192.0.2.1 g 233.252.0.1 r 192.0.2.2
(config)#no ip msdp sa s 192.0.2.1 g 233.252.0.1
```

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 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
```

p 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
```

© 2026 IP Infusion Inc. Proprietary

ip pim bfd

Use this command to enable PIMv4 BFD on an interface.

Use the `no` option with this command to revert to default.

Command Syntax

```
ip pim bfd (disable|)
no ip pim bfd
```

Parameters

`disable`	Useful when PIMv4 BFD is enabled at global level (refer command i`p pim bfd all-interfaces`) and it is required to disable `pim bfd` on a particular interface.

Default

By default, PIMv4 BFD is disabled on the interface.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#interface eth0
(config-if))#ip pim bfd
(config-if)#ip pim bfd disable
(config-if)#no ip pim bfd
```

ip pim bfd all-interfaces

Use this command to enable PIMv4 BFD on all the interfaces of a VRF instance.

Use the `no` option with this command to revert to default.

Command Syntax

```
ip pim (vrf NAME|) bfd all-interfaces
no ip pim (vrf NAME|) bfd all-interfaces
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.

Default

By default, PIMv4 BFD is disabled on all interfaces.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#ip pim bfd all-interfaces
(config)#no ip pim bfd all-interfaces

#configure terminal
(config)#ip pim vrf TEST_VRF bfd all-interfaces
```

ip pim bidir-enable

Use this command to enable Bidirectional PIM.

Use the no option with this command to disable Bidirectional PIM.

Command Syntax

```
ip pim bidir-enable
no ip pim bidir-enable
```

Parameters

None

Default

By default, bidirectional pim is disabled.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-enable

#configure terminal
(config)#no ip pim bidir-enable
```

ip pim bidir-offer-interval

Use this command to configure the bidirectional pim designated forwarder (DF) election offer message interval time. Time interval default unit is seconds.

Use the no command to revert the offer interval period configuration to the default value.

Command Syntax

```
ip pim bidir-offer-interval <1-20000> (msec|)
no ip pim bidir-offer-interval
```

Parameters

msec	Specify interval time in milliseconds

Default

The default value for interval time is 100 ms.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-offer-interval 123 msec
(config)#no ip pim bidir-offer-interval
```

ip pim bidir-offer-limit

Use this command to configure the number of unanswered offers before the device changes the interface state to the designated forwarder (DF) Winner

Use the no command to reset the offer limit to its default

Command Syntax

```
ip pim bidir-offer-limit <4-100>
no ip pim bidir-offer-limit
```

Parameters

<4-100>	Specify the limit of unanswered offers.

Default

The default value is three unanswered offers.

Command Mode

Global mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip pim bidir-offer-limit 50
(config)#no ip pim bidir-offer-limit
```

ip pim bidir-neighbor-filter

Use this command to specify which BIDIR neighbors to be considered in DF election.

Use the `no` form of this command to allow all BIDIR neighbors to take place in DF election.

Command Syntax

```
ip pim bidir-neighbor-filter WORD
no ip pim bidir-neighbor-filter
```

Parameters

`WORD`	Name of an BIDIR peering filter

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip pim bidir-neighbor-filter acl1
(config-if)#no ip pim bidir-neighbor-filter
```

ip pim bind ecmp-bundle

Use this command to bind interfaces to an ECMP bundle.

Use the no option with this command to unbind the interfaces from an ECMP bundle.

Command Syntax

```
ip pim bind ecmp-bundle WORD
no ip pim bind ecmp-bundle
```

Parameters

WORD	ECMP bundle name

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip pim bind ecmp-bundle ebund1
(config)#commit
(config)#no ip pim bind ecmp-bundle
(config)#commit
```

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 xe1
(config-if)#ip pim bsr-border

(config)#interface xe1
(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 (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>
ip pim (vrf NAME|) bsr-candidate IFNAME
no ip pim (vrf NAME|) bsr-candidate
```

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 xe1 20 30
(config)#ip pim bsr-candidate xe1
(config)#no ip pim bsr-candidate
```

ip pim crp-cisco-prefix

Use this command to turn on or turn the Candidate-RP debugging timer-working with Cisco BSR.

Use the no form of this command to turn off the Candidate-RP debugging timer-working with Cisco BSR.

Command Syntax

```
ip pim crp-cisco-prefix
no ip pim crp-cisco-prefix
```

Parameters

`crp-cisco-prefix`

Candidate-RP debugging timer-working with Cisco BSR.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim crp-cisco-prefix
(config)#no ip pim crp-cisco-prefix
```

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
```

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 xe1
(config-if)#ip pim dr-priority 11234

(config)#interface xe1
(config-if)#no ip pim dr-priority
```

ip 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

```
ip pim (vrf NAME|) ecmp-bundle WORD
no ip pim (vrf NAME|) ecmp-bundle WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	ECMP bundle name

Default

.None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip pim ecmp-bundle ebund1
(config)#commit
(config)#no ip pim ecmp-bundle ebund1
(config)#commit
```

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 xe1
(config-if)#ip pim exclude-genid

(config)#interface xe1
(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 xe1
(config-if)#ip pim hello-holdtime 123

(config)#interface xe1
(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 xe1
(config-if)#ip pim hello-interval 123

(config)#interface xe1
(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 (vrf NAME|) jp-timer <1-65535>
no ip pim (vrf NAME|) jp-timer
```

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
```

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
```

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

```
(config)#interface xe1
(config-if)#ip pim neighbor-filter xyz
(config-if)#commit
(config-if)#no ip neighbor-filter
(config-if)#commit
(config-if)#
```

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 xe1
(config-if)#ip pim dense-mode passive

(config)#interface xe1
(config-if)#no ip pim dense-mode passive

#configure terminal
(config)#interface xe1
(config-if)#ip pim sparse-mode passive

(config)#interface xe1
(config-if)#no ip pim sparse-mode passive
```

© 2026 IP Infusion Inc. Proprietary

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 1000 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip pim propagation-delay 1000

(config)#interface xe1
(config-if)#no ip pim propagation-delay
```

ip pim redundancy

Use this command to set the priority for which a router is elected as the designated router (DR).

Use the `no` form of this command to unset the configured priority.

Note: This command should be applied to the all related VRRP routers with identical priority values

Command Syntax

```
ip pim redundancy <1-255> vrrp dr-priority <0-4294967294>
no ip pim redundancy vrrp
```

Parameter

`<1-255>`	VRRP virtual router identifier
`<0-4294967294>`	DR priority

Default

None.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim redundancy 1 vrrp dr-priority 900
(config)#interface eth0
(config-if)#no ip pim redundancy vrrp
```

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 (vrf NAME|) register-rate-limit <1-65535>
no ip 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

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.

Command Syntax

```
ip pim (vrf NAME|) register-rp-reachability (disable|enable)
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 disable
(config)#no ip register-rp-reachability
(config)#commit
```

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 (vrf NAME|) register-source (A.B.C.D|IFNAME)
no ip pim (vrf NAME|) register-source
```

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

```
(config)#ip pim register-source 3.3.3.2
(config)#no ip register-source
```

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 <11-65535>
ip pim (vrf NAME|) register-suppression <11-65535>
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
`<11-65535>`	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
```

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
```

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 (vrf NAME|) rp-address A.B.C.D (override|)
ip pim (vrf NAME|) rp-address A.B.C.D WORD
ip pim (vrf NAME|) rp-address A.B.C.D WORD override bidir
no ip pim (vrf NAME|) rp-address A.B.C.D WORD override bidir
no ip pim (vrf NAME|) rp-address A.B.C.D bidir
no ip pim (vrf NAME|) rp-address A.B.C.D (override|)
no ip pim (vrf NAME|) rp-address A.B.C.D WORD
```

Parameters

`bidir`	Bidirectional RP address
`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Standard Access-list name
`override`	Static RP overrides dynamically-learned RP

Default

No PIM static group-to-RP mappings are configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#ip pim rp-address 192.168.100.1 override
(config)#ip pim rp-address 3.3.3.3 xyz
(config)#ip pim rp-address 2.2.2.2 ip1 bidir
(config)#ip pim rp-address 192.168.0.1 abc override bidir
(config)#no ip pim rp-address 192.168.0.1 abc override bidir
(config)#no ip pim rp-address 192.168.100.1 override
(config)#no ip pim rp-address 192.168.0.1 bidir
```

ip pim rp-candidate

Use this command to give the router a candidate RP status using the IP address of the specified interface.

Use the no option along with this command to remove the settings.

Command Syntax

```
ip pim rp-candidate IFNAME (bidir|) (group-list WORD|) (interval <0-16383>|)
  (priority <0-255>|)
ip pim (vrf NAME) rp-candidate IFNAME (bidir|) (group-list WORD|) (interval <0-
  16383>|) (priority <0-255>|)


ip pim (vrf NAME|) rp-candidate IFNAME bidir
no ip pim (vrf NAME|) rp-candidate IFNAME bidir
```

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 xe1
(config)#ip pim rp-candidate xe1 bidir
(config)#no ip pim rp-candidate xe1 bidir
```

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 xe1
(config-if)#ip pim state-refresh origination-interval 65

(config)#interface xe1
(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 xe1
(config-if)#ip pim unicast-bsm

(config)#interface xe1
(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
```

© 2026 IP Infusion Inc. Proprietary

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
```

© 2026 IP Infusion Inc. Proprietary

show ip msdp peer

Use this command to display information about a Multicast Source Discovery Protocol (MSDP) peer.

Command Syntax

```
show ip msdp peer (A.B.C.D|)
show ip msdp (vrf NAME|) peer (A.B.C.D|)
```

Parameters

A.B.C.D	IPv4 address of peer
NAME	Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#show ip msdp peer

MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

Table 1-1: show ip msdp peer output

Entry	Description
MSDP Peer	IP address of the peer
Connection status	State – Up, Down, Invalid, Disabled, Inactive, Listening, Connecting, Established, or Maximum. Keepalive sent – Keepalive messages sent to peer. Keepalive received – Keepalive messages received from the peer. number of connect retries – Number of peer connect retries.

show ip msdp sa-cache

Use this command to display the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

You can specify zero, one, or two addresses:

- If you do not specify any address, the entire Source-Active (SA) cache is displayed.
- If you specify only a unicast address it is treated as a source; if you specify only a multicast address it is treated as a group. In either case, entries corresponding to that address are displayed.
- If you specify two addresses, an (S, G) entry corresponding to those addresses is displayed; one address must be unicast and the other address must be multicast.

Command Syntax

```
show ip msdp sa-cache
show ip msdp sa-cache details
show ip msdp sa-cache A.B.C.D
show ip msdp sa-cache A.B.C.D A.B.C.D
show ip msdp (vrf NAME|) sa-cache
show ip msdp (vrf NAME|) sa-cache details
show ip msdp (vrf NAME|) sa-cache A.B.C.D
show ip msdp (vrf NAME|) sa-cache A.B.C.D A.B.C.D
```

Parameters

`A.B.C.D`	Source and/or group IP address
`details`	Detailed sa-cache information
`NAME`	Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02
Exptime  00:03:28P
```

Table 1-2: show ip msdp sa-cache output

Entry	Description
MSDP Source-Active Cache	• (S,G) address pair – Source address, multicast address • RP – Reverse Path address • RRF-Peer – Reverse Path Forwarding address • Uptime – as stated • Exptime – Time until entry timeout

show ip pim ecmp-bundle

Use this command to display PIM ECMP bundle information.

Command Syntax

```
show ip pim ecmp-bundle (WORD|)
```

Parameters

WORD	Specify the bundle name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#show ip pim ecmp-bundle
Name        : dn_str_rtrs_bundle_1
Interface   : <ECMP REDIRECT status>
        xe7 : allowed
        xe8 : allowed
```

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
```

Note: For `show ip pim (vrf NAME|) interface detail` command:

- Output shall contain '**Bidirectional Forwarding Detection is enabled**' in case PIMv4 BFD is enabled on an interface either by global command or at interface level.
- Output shall contain '**Bidirectional Forwarding Detection is disabled**' in case PIMv4 BFD is explicitly disabled on an interface.

Table 1-3: Show ip pim interface output

Entry	Description
Address	IP address of the interface
Interface	Interface name (eth1, xe3, ge4/1, etc.).
VIFindex	The index number of the Virtual Host Interface (vif).
Ver/Mode	PIM version (either v1, v2, or v3) / PIM Mode – Either S (sparse mode) or D (dense mode).
Nbr Count	Neighbor Count.
DR Prior	Designated Router Priority.
DR	Address of the Designated Router.
Hello Period	Routing devices send hello messages at a fixed interval on all PIM-enabled interfaces. By using hello messages, routing devices advertise their existence as PIM routing devices on the subnet.
Next Hello	When the interval counts down to 0, the routing device sends another hello message, and the timer is reset. A routing device that receives no response from a neighbor in 3.5 times the interval value drops the neighbor.
Propagation Delay	Vif Hello LAN Delay – propagation delay in milliseconds.
ECMP Redirect, bundle	An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.
Neighbors	A list of the addresses of PIM multicast neighbors.

show ip pim interface df

Use this command to display Bidirectional-PIM Designated Forwarder(DF) election status.

Command Syntax

```
show ip pim interface (IFNAME|) df (A.B.C.D|)
```

Parameters

IFNAME	Name of the interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
Router# show ip pim interface df

Interface RP          DF Winner   Metric
eth1      10.10.0.2   10.4.0.2    0
          10.10.0.3   10.4.0.3    0
          10.10.0.5   10.4.0.4    409600
eth2      10.10.0.2   10.5.0.2    0

Router# show ip pim interface eth1 df 10.10.0.3

Designated Forwarder election for eth1, 10.4.0.2, RP 10.10.0.3
   State Non-DF
   Offer count is 0
   Current DF ip address 10.4.0.3
   Last winner metric preference 0
   Last winner metric 0
```

show ip pim mroute

Use this command to display information in the IP PIM multicast routing table.

Command Syntax

```
show ip pim mroute (detail|)
show ip pim mroute A.B.C.D (detail|)
show ip pim mroute A.B.C.D E.F.G.H (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 E.F.G.H (detail|)
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`E.F.G.H`	Display all entries for this group IP address
`A.B.C.D`	Display all entries for this source IP address

Note: An IP address cannot be a group address and a source address at the same time.

`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 1-4: 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
```

Note: For `show ip pim (vrf NAME|) neighbor detail` command:

- Output shall contain '**Bidirectional Forwarding Detection is enabled**' in case PIMv4 BFD detection is enabled for this neighbor.

Table 1-5: 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 1-5: Show ip pim neighbor output

Entry	Description
Lan delay:	In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: neighbor.lan_prune_delay_present A flag indicating if the LAN Prune Delay option was present in the Hello message. neighbor.tracking_support A flag storing the value of the T bit in the LAN Prune Delay option if it is present in the Hello message. This indicates the neighbor's capability to disable Join message suppression. neighbor.propagation_delay The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message. neighbor.override_interval The Override_Interval field of the LAN Prune Delay option (if present) in the Hello message. The additional state described above is deleted along with the DR neighbor state when the neighbor timeout expires.
Override interval:	Hello Override Interval
DR priority:	The DR_Priority Option allows a network administrator to give preference to a particular router in the DR election process by giving it a numerically larger DR Priority.The DR_Priority Option SHOULD be included in every Hello message, even if no DR Priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR_Priority Option. The default priority is 1.
Gen ID:	Generation Identifier, used to detect reboots.
Interface ID:	As stated.
Router-ID:	As stated.
Local-ID:	As stated.
ECMP REDIRECT	Whether ECMP Redirect is enabled or disabled.

show ip pim nexthop

Displays the nexthop information from NSM as used by PIM.

Command Syntax

```
show ip pim nexthop
show ip pim (vrf NAME|) nexthop
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim nexthop
```

show ip pim bsr-router

Use this command to show the bootstrap router PIMv2 address.

Command Syntax

```
show ip pim bsr-router
show ip pim (vrf NAME|) bsr-router
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 10.10.11.35 (?)
  Uptime:      00:00:38, BSR Priority: 0, Hash mask length: 10
  Expires:     00:01:32
  Role: Non-candidate BSR
  State: Accept Preferred

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

Table 1-6: 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 1-6: Show ip pim bsr-router output (Continued)

Entry	Description
Role	Specifies whether the BSR is the Candidate BSR or a Non-candidate BSR
State	• The current state of a Candidate BSR, one of the following: Candidate-BSR, Pending-BSR, or Elected-BSR. • The current state of a Non-candidate BSR, one of the following: Accept Any or Accept Preferred.

show ip pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax

```
show ip pim local-members
show ip pim local-members IFNAME
show ip pim (vrf NAME|) local-members
show ip pim (vrf NAME|) local-members IFNAME
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Display local membership for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim vrf q local-members p8p1
PIM Local membership information

p8p1:
  (*, 233.5.5.5) : Include
  (*, 233.7.7.7) : Include
```

Table 1-7: Show ip pim local-members output

Entry	Description
NAME:	Interface name
(*,G)	The local members in the form (Source/Group). Shows state – either Include or Exclude.

show ip pim rp-hash

Use this command to display the rendezvous point (RP) to chose based on the group selected.

Command Syntax

```
show ip pim rp-hash A.B.C.D
show ip pim (vrf NAME|) rp-hash A.B.C.D
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

A.B.C.D in command refers to the group address to be hashed.

```
#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

Table 1-8: 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 1-9: 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
```

CHAPTER 2 PIMv6 Commands

This chapter describes the commands for Protocol-Independent Multicast (PIM).

Note: Supported only in Qumran2 platforms.

- clear ipv6 mroute
- clear ipv6 pim sparse-mode bsr
- debug ipv6 pim
- debug ipv6 pim packet
- debug ipv6 pim timer assert
- debug ipv6 pim timer bsr
- debug ipv6 pim timer hello
- debug ipv6 pim timer joinprune
- debug ipv6 pim timer register
- ipv6 pim
- ipv6 pim accept-register
- ipv6 pim anycast-rp
- ipv6 pim bfd
- ipv6 pim bfd all-interfaces
- ipv6 pim bind ecmp-bundle
- ipv6 pim bsr-border
- ipv6 pim bsr-candidate
- ipv6 pim cisco-register-checksum
- ipv6 pim crp-cisco-prefix
- ipv6 pim dr-priority
- ipv6 pim ecmp-bundle
- ipv6 pim exclude-genid
- ipv6 pim hello-holdtime
- ipv6 pim hello-interval
- ipv6 pim ignore-rp-set-priority
- ipv6 pim jp-timer
- ipv6 pim neighbor-filter
- ipv6 pim passive
- ipv6 pim propagation-delay
- ipv6 pim register-rate-limit
- ipv6 pim register-rp-reachability
- ipv6 pim register-source
- ipv6 pim register-suppression
- ipv6 pim router-id

© 2026 IP Infusion Inc. Proprietary

- ipv6 pim rp-address
- ipv6 pim rp-candidate
- ipv6 pim rp embedded
- ipv6 pim rp-register-kat
- ipv6 pim spt-threshold
- ipv6 pim ssm
- ipv6 pim state-refresh origination-interval
- ipv6 pim unicast-bsm
- show debugging ipv6 pim
- show ipv6 pim bsr-router
- show ipv6 pim ecmp-bundle
- show ipv6 pim interface
- show ipv6 pim mroute
- show ipv6 pim neighbor
- show ipv6 pim nexthop
- show ipv6 pim local-members
- show ipv6 pim rp-hash
- show ipv6 pim rp mapping

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
  (assert|bsr|hello|joinprune|register|)|)
debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state
  |timer (assert|bsr|hello|joinprune|register|)|)
no debug ipv6 pim (all|events|mfc|mib|mtracenexthop|nsm|packet|state|timer
  (assert|bsr|hello|joinprune|register|)|)
no debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtracenexthop|nsm|packet
  |state|timer (assert|bsr|hello|joinprune|register|)|)
```

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
`assert`	Enable debugging for assert timers
`bsr`	Enable debugging for BSR timers
`hello`	Enable debugging for hello timers
`joinprune`	Enable debugging for joinprune timers
`register`	Enable debugging for register timers

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 6.2.0.

Examples

```
(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 (vrf NAME|) timer assert
no debug ipv6 pim timer assert
no debug ipv6 pim (vrf NAME|) timer assert
```

Parameters

`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 and updated in OcNOS version 6.2.0.

Example

```
#debug ipv6 pim timer assert
```

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 (vrf NAME|) timer register
no debug ipv6 pim timer register
no debug ipv6 pim (vrf NAME|) timer register
```

Parameters

`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

```
#debug ipv6 pim timer register
```

ipv6 pim

Use this command to enable IPv6 PIM dense-mode or sparse-mode on the current interface.

Use the `no` option with this command to disable IPv6 PIM dense-mode or sparse-mode on the interface.

Command Syntax

```
ipv6 pim (dense-mode|sparse-mode|)
no ipv6 pim (dense-mode|sparse-mode|)
```

Parameters

`dense-mode`	Enable IPv6 PIM dense-mode operation
`sparse-mode`	Enable IPv6 PIM sparse-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-mode

(config-if)#no ipv6 pim sparse-mode
```

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 (vrf NAME|) accept-register list WORD
no ipv6 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

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 bfd

Use this command to enable PIMv6 BFD on an interface.

Use the `no` option with this command to revert to default.

Command Syntax

```
ipv6 pim bfd (disable|)
no ipv6 pim bfd
```

Parameters

`disable`	Useful when PIMv6 BFD is enabled at global level (refer command `ipv6 pim bfd all-interfaces`) and it is required to disable PIMv6 BFD on a particular interface.

Default

By default, PIMv6 BFD is disabled on the interface.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 pim bfd
(config-if)#ipv6 pim bfd disable
(config-if)#no ipv6 pim bfd
```

ipv6 pim bfd all-interfaces

Use this command to enable PIMv6 BFD on all the interfaces of a VRF instance.

Use the `no` option with this command to revert to default.

Command Syntax

```
ipv6 pim (vrf NAME|) bfd all-interfaces
no ipv6 pim (vrf NAME|) bfd all-interfaces
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.

Default

By default, PIMv6 BFD is disabled on all interfaces.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#ipv6 pim bfd all-interfaces
(config)#ipv6 pim vrf TEST_VRF bfd all-interfaces
(config)#no ipv6 pim bfd all-interfaces
(config)#no ipv6 pim vrf TEST_VRF bfd all-interfaces
```

© 2026 IP Infusion Inc. Proprietary

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
```

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
```

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 (vrf NAME|) bsr-candidate IFNAME
no ipv6 pim (vrf NAME|) bsr-candidate
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Specify the name of the interface

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim bsr-candidate eth0
(config)#no ipv6 pim bsr-candidate
```

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 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
```

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
```

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 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 (vrf NAME|) jp-timer <1-65535>
no ipv6 pim (vrf NAME|) jp-timer
```

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
```

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 WORD
no ipv6 pim neighbor-filter
```

Parameters

`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)#no ipv6 neighbor-filter
```

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
```

© 2026 IP Infusion Inc. Proprietary

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 <0-32767>
no ipv6 pim propagation-delay
```

Parameter

<0-32767>	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 1000 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 (vrf NAME|) register-rate-limit <1-65535>
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/disable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to the default state.

Command Syntax

```
ipv6 pim (vrf NAME|) register-rp-reachability (disable|enable)
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

```
(config)#ipv6 pim register-rp-reachability enable
(config)#commit
(config)#ipv6 pim register-rp-reachability disable
(config)#commit
(config)#no 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 (vrf NAME|) register-source (X:X::X:X |IFNAME)
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 (vrf NAME|) register-suppression <11-65535>
no ipv6 pim (vrf NAME|) register-suppression
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<11-65535>`	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
```

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
```

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 (vrf NAME|) rp-address X:X::X:X (override|)
no ipv6 pim (vrf NAME|) rp-address X:X::X:X (override|)
```

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
`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 override

#configure terminal
(config)#no ipv6 pim rp-address 30:30:5::153 override
```

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 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 (disable|enable)
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 enable
(config)#ipv6 pim rp embedded disable
(config)#no ipv6 pim rp embedded
```

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
```

© 2026 IP Infusion Inc. Proprietary

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 2-18 explains the fields for each pim entry.

Table 2-1: show ipv6 pim bsr-router

Entry	Description
BSR address	Address of the Bootstrap router (BSR).
Uptime	As Stated.
BSR Priority	The current priority of the BSR (this is configurable).
Hash mask length	For Rendezvous Point (RP) addresses in the matching group-range-to-RP mappings, compute a value — Value(G,M,C(i))= (1103515245 * ((1103515245 * (G&M)+12345) XOR C(i)) + 12345) mod 2^31 where C(i) is the RP address and M is a hash-mask.
Next bootstrap message	Time until next boostrap message.
Role	AS stated..

Table 2-1: show ipv6 pim bsr-router

Entry	Description
State	As stated..
Candidate RP	Address of the rendezvous point (RP).
Advertisement interval	As stated.
Next C-RP advertisement	Time before the next Candidate RP is advertised.

show ipv6 pim ecmp-bundle

Use this command to display IPv6 PIM ECMP bundle information.

Command Syntax

```
show ipv6 pim ecmp-bundle (WORD|)
```

Parameters

WORD	Specify the bundle name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#show ipv6 pim ecmp-bundle
Name        : upstr_bundle_1
Interface   : <ECMP REDIRECT status>
        ce9 : allowed
       ce10 : allowed
```

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
```

© 2026 IP Infusion Inc. Proprietary

Table 2-19 explains the fields for each pim entry.

Note: For `show ipv6 pim (vrf NAME|) interface detail` command:

- Output shall contain '**Bidirectional Forwarding Detection is enabled**' in case PIMv6 BFD is enabled on an interface either by global command or at interface level.
- Output shall contain '**Bidirectional Forwarding Detection is disabled**' in case PIMv6 BFD is explicitly disabled on an interface.

Table 2-2: 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 2-20 explains the fields for each pim entry.

Table 2-3: 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 2-3: (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 2-21 explains the fields for each pim entry.

Note: For `show ipv6 pim (vrf NAME|) neighbor detail` command:

- Output shall contain '**Bidirectional Forwarding Detection is enabled**' in case PIMv6 BFD detection is enabled for this neighbor.

Table 2-4: 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.

© 2026 IP Infusion Inc. Proprietary

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 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 2-22 explains the fields for each pim entry.

Table 2-5: 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 2-23 explains the fields for each pim entry.

Table 2-6: 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:
```

Multicast Listener Discovery Configuration

CHAPTER 1 MLD Configuration

Overview

Multicast Listener Discovery (MLD) is a protocol used by IPv6 hosts to communicate their desire to receive multicast traffic to the neighboring multicast routers. It serves a role similar to that of Internet Group Management Protocol (IGMP) in IPv4 networks. MLD is essential for efficient multicast routing in IPv6 networks, ensuring that multicast data is only sent to network segments with interested receivers.

IP hosts use MLD to inform multicast routers about their membership in specific multicast groups, allowing routers to maintain a list of group memberships per interface. When a host joins a multicast group, it sends an MLD Report to the router, which updates its membership list. Routers then use this information to forward multicast data only to network segments with interested hosts, optimizing network resources by preventing unnecessary traffic.

By default, when PIMv6 is enabled on an interface, MLD version 2 is enabled. MLD can be enabled on an interface explicitly.

Feature Characteristics

MLD allows hosts to notify multicast routers about their interest in joining or leaving multicast groups, with routers maintaining membership lists for each interface. Hosts use MLD Report messages to join and Done messages to leave groups, enabling routers to update memberships. Routers then use this data to forward multicast traffic only to interested network segments, optimizing bandwidth. By default, MLDv2 is enabled with PIMv6, supporting source-specific multicast and maintaining compatibility with MLDv1. Administrators can manually configure MLD on interfaces as needed, ensuring effective multicast management and interoperability between versions.

Benefits

These benefits make MLD an essential protocol for efficient and effective multicast routing in IPv6 networks, enhancing performance, scalability, and resource utilization.

- Efficient Multicast Traffic Management
- Network Resource Optimization
- Improved Scalability
- Enhanced Performance and Reliability
- Compatibility and Interoperability
- Administrative Control and Flexibility.

MLD Versions

OcNOS supports MLDv1 and MLDv2. By default, OcNOS enables MLDv2 when PIMv6 is enabled on an interface.

MLDv2 includes the following key changes from MLDv1:

- 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.

© 2026 IP Infusion Inc. Proprietary

    - The multicast state that is maintained for groups and sources, not just for groups as in MLDv1.
- Hosts no longer perform report suppression, which means that hosts always send MLD membership reports when an MLD query message is received.

MLD Operation

MLD works on the premise of three major packets exchange between MLD enabled routers and hosts, interested in joining a particular group.

MLD Query Operation

Once MLD is enabled or PIMv6 is enabled (which enables MLDv2), on any interface it starts sending Query message, which is called general query to the all-hosts multicast group at ff02::1 periodically to discover whether any hosts want to receive multicast data.

OcNOS elects a router as the MLD 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 IPv6 link local address is less than Router-2 eth2, Router-1 eth2 becomes querier on the LAN.

MLD 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 MLD group table containing multicast group-address, interface name on which it receives the report.

MLD Leave Operation

When a multicast host leaves a group, a host that runs MLD sends an MLD leave message. To check if this host is the last host to leave the group, the router sends an MLD 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 MLD table.

Configuration

You can configure MLD on a network device to manage multicast group memberships effectively. This configuration enables efficient multicast traffic distribution, optimizes bandwidth usage, and ensures that multicast data is only sent to network segments with interested receivers.

Topology

This topology ensures that each router's interfaces are configured with the specified IP or IPv6 link-local addresses, and verifies the switch's configurations for connectivity. It involves setting up routing protocols or static routes on each router for communication, and assigning and configuring IPv6 addresses on router and host interfaces to ensure proper device communication via link-local addresses. Additionally, routers are configured to handle unicast or multicast traffic, with necessary multicast routing protocols set up for multicast traffic.

The network topology shown in the Figure 1-13 includes three routers, a switch, two hosts, and a source.

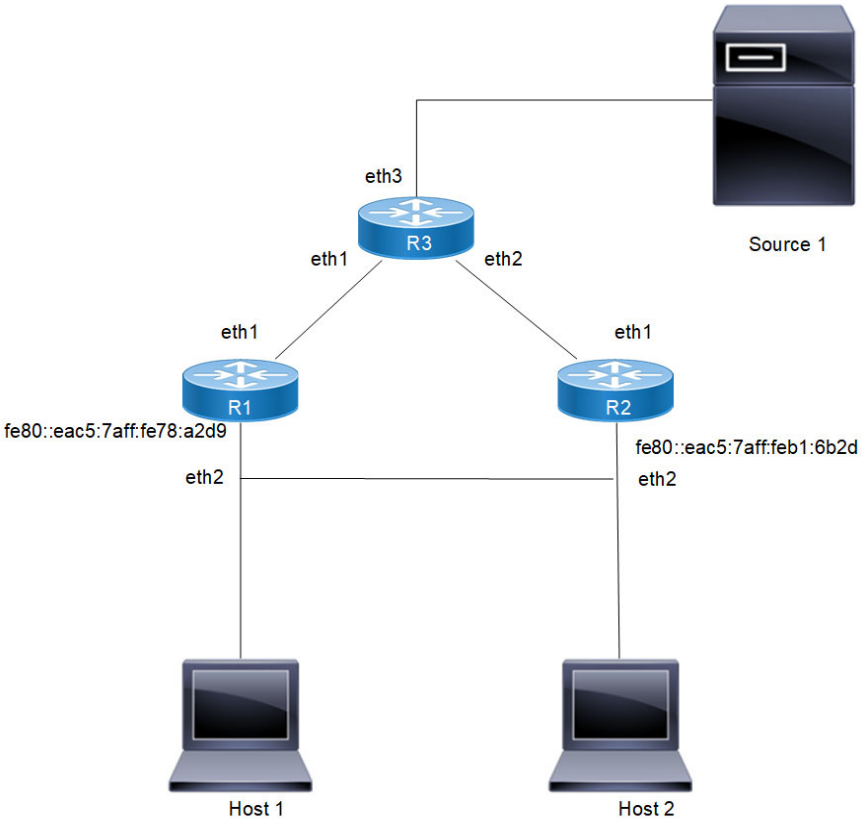


Figure 1-1: MLD Topology

Configuration

MLD Configuration

Configure Multicast Listener Discovery (MLD) on a network device. Activate MLD version 1 on the interface, which is responsible for managing the multicast group memberships.

```
R1#configure terminal
R1(config)#ipv6 multicast-routing
R1(config)#interface eth2
R1(config-if)#ip address 2001::1/64
R1(config-if)#ipv6 mld version 1
R1(config-if)#commit
R1(config-if)#exit
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
#show  running-config
!
no service password-encryption
!
hostname rtr1
!
Ipv6 multicast-routing
!
!
interface eth2
ip address 2001::1/64
no shutdown
ipv6 mld version 1
```

Configuring MLD Parameters

The configuration that follows shows how MLD parameters can be configured.

1. Assign the IPv6 address 2001::1/64 to the eth2 interface, enabling IPv6 communication.

   ```
   R1#configure terminal
   R1(config)#interface eth2
   R1(config-if)#ip address 2001::1/64
   ```

2. Enable MLD Immediate Leave that allows the interface to immediately remove a host from a multicast group when it sends a leave message, improving the efficiency of multicast group management..

   ```
   R1(config-if)#ipv6 mld version 1
   R1(config)#ipv6 multicast-routing
   R1(config)#interface eth2
   R1(config-if)#ipv6 mld access-group 1
   R1(config-if)#ipv6 mld immediate-leave
   ```

3. Configure MLD group-list. This command associates a specific group-list (1) with the MLD configuration, controlling which multicast groups are permitted on the interface. Set the MLD querier timeout, interval, query maximum response time, robustness variable, startup query count, and startup query interval.

   ```
   R1(config-if)#group-list 1
   R1(config-if)# ipv6 mld  last-member-query-count 7
   R1(config-if)# ipv6 mld  last-member-query-interval 25500
   ```

```
R1(config-if)#ipv6 mld limit 100
R1(config-if)#ipv6 mld querier-timeout 300
R1(config-if)#ipv6 mld  query-interval 200
R1(config-if)#ipv6 mld  query-max-response-time 150
R1(config-if)#ipv6 mld  robustness-variable 4
R1(config-if)#ipv6 mld startup-query-count 4
R1(config-if)# ipv6 mld startup-query-interval 50
R1(config-if)#ipv6 mld static-group  FF1E::1
R1(config-if)#commit
R1(config-if)#exit
```

Validation

Enter the commands listed in this section to confirm the previous configurations

```
#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
Ipv6 multicast-routing
!
!
interface eth2
 ipv6 address 2001::1/64
 no shutdown
 ipv6 mld access-group 1
 ipv6 mld immediate-leave group-list 1
 ipv6 mld last-member-query-count 7
 ipv6 mld limit 100
 ipv6 mld static-group ff1e::1
 ipv6 mld last-member-query-interval 25500
 ipv6 mld querier-timeout 300
 ipv6 mld query-interval 200
 ipv6 mld query-max-response-time 150
 ipv6 mld startup-query-interval 50
 ipv6 mld startup-query-count 4
 ipv6 mld robustness-variable 4
 ipv6 mld ra-option
 ipv6 mld version 1
 !!

Rtr1#show ipv6 mld interface eth2
Interface eth2 (Index 4)
MLD Enabled, Active, Querier, Configured for version 1
 Internet address is fe80::eac5:7aff:fe78:a2d9
 MLD interface limit is 100
 MLD interface has 1 group-record states
 MLD interface statistics:
 v1-reports: 0, v1-leaves: 0
```

```
v2-reports: 0
MLD query interval is 200 seconds
MLD startup query interval is 50 seconds
MLD startup query count is 4
MLD querier timeout is 300 seconds
MLD max query response time is 150 seconds
Group Membership interval is 950 seconds
MLD Last member query count is 7
Last member query response interval is 1000 milliseconds
```

MLD Group Table after MLDv1 Membership Report is received:

MLD 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 ipv6 mld groups` command displays the MLD group table. In this table, the following fields are defined.

Table 1-1: MLD group table after MLDv1 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.

```
#show ipv6 mld groups
MLD Connected Group Membership
Group Address         Interface         Uptime    Expires   State    Last Reporter
ff04::1                 xe18           00:00:10   00:15:40 Active   fe80::1
ff1e::1                 xe18           00:17:22   static   Active   ::

#show ipv6 mld groups detail
MLD Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      xe18
Group:          ff04::1
Flags:          R
Uptime:         00:00:33
Group mode:     Exclude (Expires: 00:15:17)
State:          Active
Last reporter:  fe80::1
Source list is empty

Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      xe18
Group:          ff1e::1
```

```
Flags:          SG
Uptime:         00:17:45
Group mode:     Exclude (Static)
State:          Active
Last reporter:  ::
Source list is empty
```

Validation For MLDV2

```
#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
Ipv6 multicast-routing
!
!
interface eth2
 ipv6 address 2001::1/64
 ipv6 mld access-group 1
 ipv6 mld immediate-leave group-list 1
 ipv6 mld last-member-query-count 7
 ipv6 mld last-member-query-interval 25500
 ipv6 mld limit 100
 ipv6 mld static-group ff1e::1
 ipv6 mld querier-timeout 300
 ipv6 mld query-interval 200
 ipv6 mld query-max-response-time 10
 ipv6 mld startup-query-interval 50
 ipv6 mld startup-query-count 4
 ipv6 mld robustness-variable 4
 ipv6 mld version 2

Rtr1#show ipv6 mld interface eth2
MLD Enabled, Inactive, Configured for version 2
 MLD interface limit is 100
 MLD interface has 1 group-record states
 MLD interface statistics:
 v1-reports: 0, v1-leaves: 0
 v2-reports: 0
 MLD query interval is 200 seconds
 MLD startup query interval is 50 seconds
 MLD startup query count is 4
 MLD querier timeout is 300 seconds
 MLD max query response time is 10 seconds
 Group Membership interval is 510 seconds
```

```
 MLD Last member query count is 7
 Last member query response interval is 25500 milliseconds
```

MLD Group Table after MLDv2 Membership Report is received:

```
#show ipv6 mld groups
MLD Connected Group Membership
Group Address     Interface  Uptime   Expires  State    Last Reporter
ff04::1            eth2      00:00:11 00:13:16 Active   fe80::200:4ff:fe71:3415
ff1e::1            eth2      00:08:05   static Active   fe80::200:4ff:fe71:3415

#show ipv6 mld groups detail
MLD Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          ff04::1
Flags:          R
Uptime:         00:00:15
Group mode:     Exclude (Expires: 00:13:13)
State:          Active
Last reporter:  fe80::200:4ff:fe71:3415
Source list is empty

Flags: (M - SSM Mapping, R - Remote,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          ff1e::1
Flags:          R         SG
Uptime:         00:08:09
Group mode:     Exclude (Expires: 00:13:13, Static)
State:          Active
Last reporter:  fe80::200:4ff:fe71:3415
Source list is empty
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
IGMP	Multicast Listener Discovery (MLD) is a protocol used in IPv6 networks that allows network devices (hosts) to inform multicast routers of their intention to receive multicast traffic.
MLD	The Internet Group Management Protocol (IGMP) is a communication protocol used in IPv4 networks to manage multicast group memberships.

CHAPTER 2 MLD 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 MLD 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.

MLD proxy can be used in such topologies instead of PIM. With MLD proxy configured, the device serves as a proxy for the downstream hosts to send MLD messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device configured with MLD proxying is a host but no longer a PIM neighbor to the upstream device.

A device with MLD 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 MLD Proxy:

Upstream interface

Also referred to as the proxy interface. A proxy interface is an interface on which MLD 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 MLD; therefore, it is also called host interface.

Downstream interface

An interface that is running MLD and in the direction contrary to the root of the multicast forwarding tree. A downstream interface acts as a router running MLD; 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.

MLD-Proxy Configuration Steps

This section provides the configuration steps for configuring MLD Proxy and example for a relevant scenario.

- Enable IPv6 multicast on each router (see Enabling IPv6 Multicast Routing)
- Enable MLD Proxy service on the upstream interface.
- Enable MLD mroute configuration on the downstream interface.
- Enable MLD 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 IPv6 addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

IIn 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 2000::1/64 and the group address is set to ff03::1.

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.

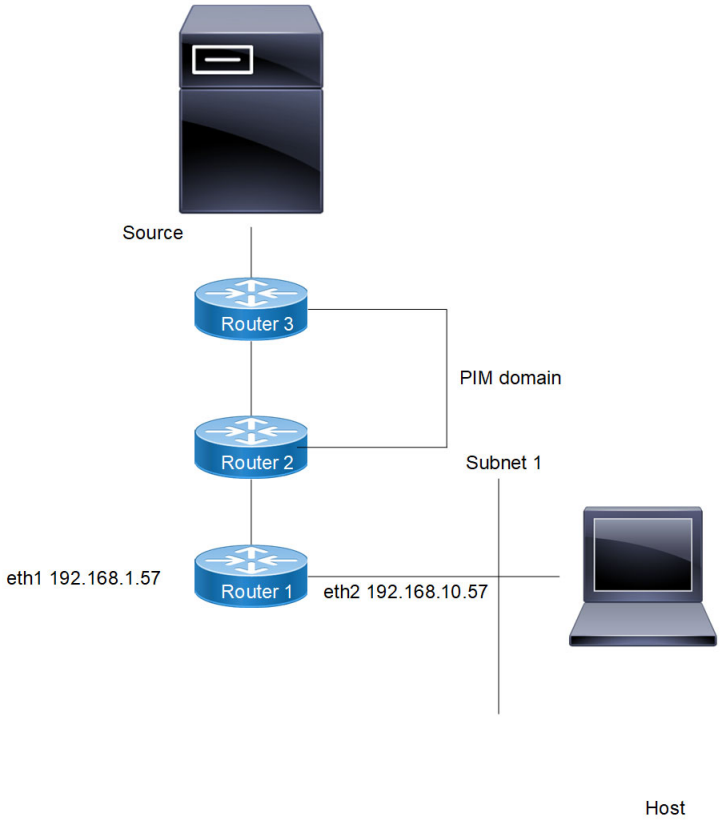


Figure 2-1: MLD Proxy Topology

In this example, Routers 2 and 3 are running PIM and Router1 is the MLD Proxying router.

- Host ends an MLD membership report to Subnet 1.
- Downstream interface on Router1 received MLD reports from host and updates the proxy interface.
- MLD 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 MLD join requested for Multicast traffic.

Enabling IPv6 Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)# ipv6 multicast-routing`	Enable IPv6 multicast routing.
`(config)#commit`	Commit the transaction.

Enabling Proxy upstream interface

Enable MLD 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 MLD host.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::1/64`	Assign IPv6 address to an interface
`(config-if)#ipv6 MLD proxy-service`	Enable MLD proxy service on the upstream interface.
`(config-if)#commit`	Commit the transaction.
`(config)#exit`	Exit Configure mode.

Enabling Proxy downstream interface

Enable MLD mroute proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Enter Interface mode
`(config-if)#ipV6 address 3000::1/64`	Assign IPv6 address to an interface
`(config-if)#ipv6 MLD mroute-proxy eth1`	Enable MLD mroute proxy on the downstream interface and specify the upstream proxy interface name.
`(config-if)#commit`	Commit the transaction.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for MLD Proxying router.

```
hostname Router1
!
interface lo
!
!
ipv6 multicast-routing
!
interface eth0
!
interface eth1
      ipv6 address 2000::1/64
      ipv6 mld proxy-service

!
interface eth2
      fec off
      ipv6 address 3000::1/64
      ipv6 mld mroute-proxy eth1

!
```

MLD proxy interface

The following output displays the mld Proxy interface information.

```
Router1#show ipv6 mld interface

Interface eth1 (Index 3)
 MLD Enabled, Active, Version 3 (default), proxy-service
 MLD host version 3
 Internet address is 2000::1
 Unsolicited Report Interval is 1000 milliseconds


Interface eth2 (Index 4)
 MLD Enabled, Active, Querier, Version 3 (default)
 MLD mroute-proxy interface is eth1
 Internet address is 3000::1
 MLD interface has 1 group-record states
MLD Interface statistics:
v1-reports: 0
v2-reports: 1, v2-leaves: 0
v3-reports: 0

MLD query interval is 125 seconds
 MLD Startup query interval is 31 seconds
 MLD Startup query count is 2
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Group Membership interval is 260 seconds
 MLD Last member query count is 2
```

```
 Last member query response interval is 1000 milliseconds
```

MLD proxy

The following output displays the mld proxy information.

```
Router1#show ipv6 mld proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1
```

MLD proxy groups

The following output displays the MLD proxy group membership information.

```
Router1#show ipv6 mld proxy groups
MLD Connected Group Membership
Group Address    Interface            State     Member state
Ff03::1           eth1                 Active    Idle
```

The `show ipv6 mroute` command displays the IPv6 multicast routing table.

```
Router1#show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface

(2000::1, ff03::1), uptime 00:01:10, stat expires 00:02:46
Owner PIM, Flags: TF
  Incoming interface: eth1
  Outgoing interface list:
     eth2 (1)
```

Enabling Unsolicited report interval

Enable MLD 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)#ipv6 MLD proxy unsolicited-report-interval 20000`	Enable MLD proxy unsolicited report interval value on the upstream interface.
`(config-if)#commit`	Commit the transaction.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for MLD Proxying router.

```
hostname Router1
!
interface eth0
!
interface eth1
ipv6 address 2000::1/64
ipv6 mld proxy-service
ipv6 mld proxy unsolicited-report-interval 20000
!
interface eth2
ipv6 address 3000::1/64
ipv6 mld mroute-proxy eth1
!
interface lo
!
!
Ipv6 multicast-routing
!
```

MLD proxy Unsolicited report interval

The following output displays the MLD proxy unsolicited report interval information.

```
Router1#show ipv6 MLD interface eth1

Interface eth1 (Index 3)
 MLD Enabled, Active, Version 3 (default), proxy-service
 MLD host version 3
 Internet address is 2000::1
 Unsolicited Report Interval is 20000 milliseconds
```

MLD proxy group with unsolicited report interval

The following output displays the MLD proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ipv6 MLD proxy groups

MLD Connected Proxy Group Membership
Group Address    Interface            State     Member state
Ff03::1            eth1                 Active    Idle
```

IPv6 Multicast Routing Table

The `show ipv6 mroute` command displays the IPv6 multicast routing table.

```
Router1#show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface
```

```
(2000::1, ff03::1), uptime 00:01:10, stat expires 00:02:46
Owner PIM, Flags: TF
  Incoming interface: eth1
  Outgoing interface list:
          eth2 (1)
```

CHAPTER 3 MLD Snooping Configuration

Overview

In IPv6 networks, Multicast Listener Discovery (MLD) Snooping plays a crucial role in optimizing multicast traffic management within Layer-2 switches. By default, without MLD, Layer-2 switches treat IPv6 multicast traffic like broadcast traffic, forwarding frames received on one interface to all others. This indiscriminate forwarding leads to unnecessary traffic across the network, impacting performance.

MLD Snooping addresses this issue by intelligently monitoring and managing multicast traffic. Here’s how it works: switches enabled with MLD Snooping analyze MLD messages exchanged between IPv6 hosts and multicast routers. Instead of flooding multicast traffic to all ports, switches learn which ports have hosts interested in specific multicast groups. They then selectively forward multicast traffic only to those ports where the interested hosts reside, significantly reducing network congestion and improving efficiency.

To enable MLD Snooping, administrators typically use the switchport command on each switch port to switch it to Layer-2 mode, allowing the switch to monitor MLD messages effectively. This approach ensures that multicast traffic is delivered only to the intended recipients, optimizing network performance and resource utilization in IPv6 environments.

Feature Characteristics

MLD Snooping enables Layer-2 switches to intelligently manage IPv6 multicast traffic by forwarding packets only to ports with active listeners for specific multicast groups, preventing unnecessary network-wide flooding. By selectively forwarding multicast traffic based on MLD messages exchanged between hosts and routers, MLD Snooping enhances overall network performance, reducing congestion and optimizing bandwidth usage. It eliminates broadcast-like behavior by maintaining a multicast group table and forwarding traffic solely to ports where interested hosts are located, akin to IPv4's IGMP Snooping. This efficient management conserves network resources, delivering packets only where there are active receivers, and reduces control plane overhead by handling just one MLD membership report per multicast group, even with multiple interested hosts.

Benefits

- Efficient Multicast Traffic Management
- Improved Network Performance
- Reduced Broadcast-Like Behavior
- Optimized Resource Utilization
- Reduced Control Plane Overhead
- Enhanced Security Features
- Compatibility and Integration.

Topology

In this topology, switch S1 configures eth1 as a multicast router port. Since MLD Snooping manages multicast traffic in bridged LAN setups, router R1 does not need to run MLD Snooping and can instead utilize any multicast protocol like PIMv6-SM. Therefore, this example focuses solely on configuring switch S1, and does not cover configuration details for router R1.

© 2026 IP Infusion Inc. Proprietary

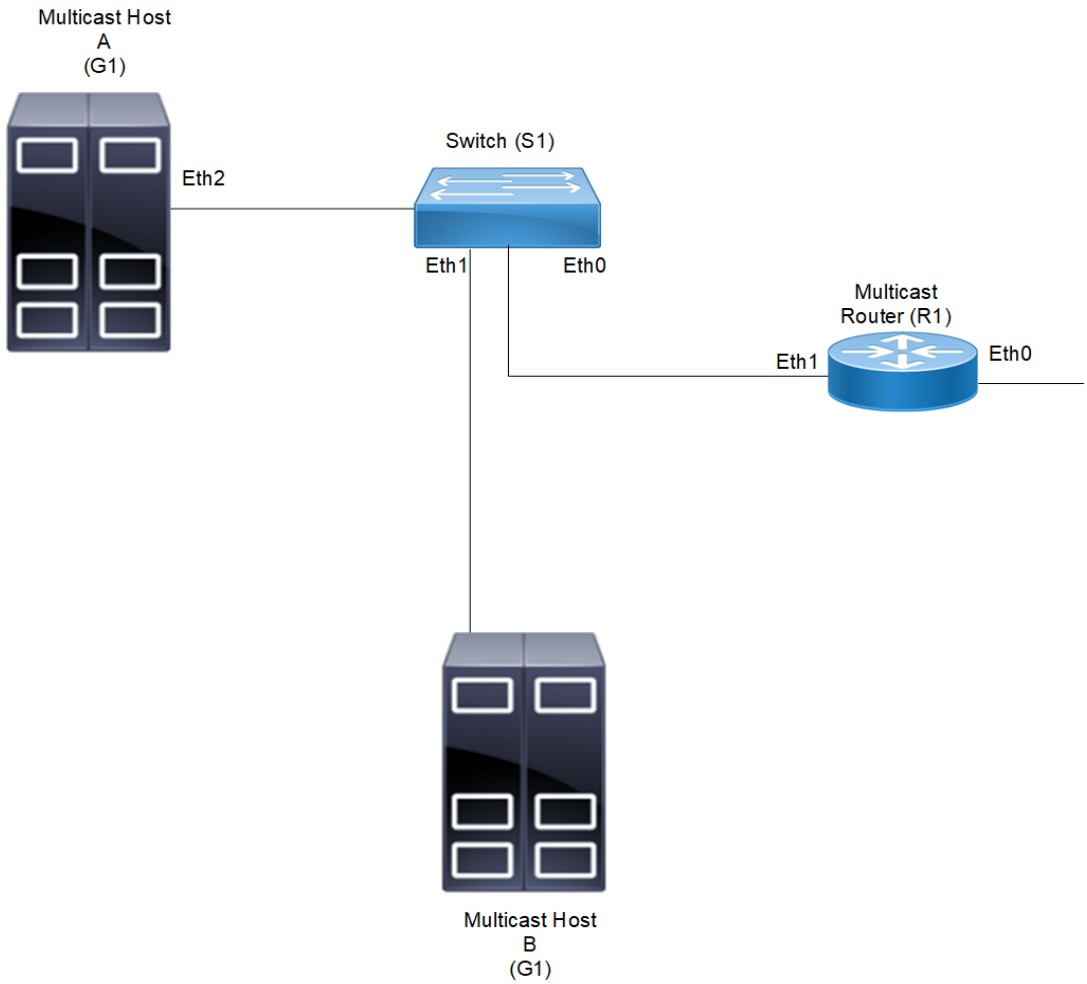


Figure 3-1: MLD Snooping Topology

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 MLD 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 MLD 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 FF02::2(All Router Destination Address).

MLD Snooping Configuration

To enable MLD 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. MLD snooping will be enabled by default

5. Configure ports that are connected to routers as multicast router ports
6. By default, MLD report suppression is enabled on the switch

Note: Execute l2 unknown mcast CLI to enable the option to drop the unknown multicast traffic.

S1

1. Enable the MLD on interface, set the bridge protocol and configure interface eth0 and access the switch port mode.

```
S1#configure terminal
S1(config)#bridge 1 protocol ieee vlan-bridge
S1(config)#interface eth0
S1(config-if)#shutdown
S1(config-if)#switchport
S1(config-if)#bridge-group 1
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
```

2. Set the bridge protocol and configure interface eth1 and access the switch port mode

```
S1(config)#interface eth1
S1(config-if)#shutdown
S1(config-if)#switchport
S1(config-if)#bridge-group 1
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
```

3. Set the bridge protocol and configure interface eth2 and access the switch port mode

```
S1(config)#interface eth2
S1(config-if)#shutdown
S1(config-if)#switchport
S1(config-if)#bridge-group 1
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
```

4. Configure interface vlan1.1 for MLD snooping.

```
S1(config)#interface vlan1.1
S1(config-if)# MLD snooping mrouter interface eth1
S1(config-if)#commit
S1(config-if)#exit
```

Validation

```
#show running-config interface eth0
!
interface eth0
```

```
switchport
bridge-group 1
switchport mode access
!
#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode access
!

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode access
!

#show mld snooping groups
MLD Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/source Address                    Interface      Flags   Uptime
Expires  Last Reporter              Version
1      ff06::2                                  eth0           R    >  00:00:41
00:03:39  fe80::1                    V2

#show mld snooping interface vlan1.1

 MLD Snooping information for vlan1.1 (Index 25001)
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Active, Non-Querier,
 MLD querying router is :
           :fe80::eac5:7aff:feb1:6b2d
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is not enabled
 MLD Snooping report suppression is enabled
 Number of Groups: 1
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 3
 Active Ports:
  eth0
eth1
eth2
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
MLD	The Internet Group Management Protocol (IGMP) is a communication protocol used in IPv4 networks to manage multicast group memberships.

Multicast Listener Discovery Command Reference

© 2026 IP Infusion Inc. Proprietary

CHAPTER 1 Layer 2 MLD Snooping Commands

This chapter describes the Layer 2 Multicast Listener Discovery (MLD) Snooping commands:

- clear mld snooping
- mld snooping
- mld snooping fast-leave
- mld snooping mrouter
- mld snooping querier
- mld snooping report-suppression
- show debugging mld snooping
- show mld snooping mrouter
- show mld snooping statistics
- show mld snooping groups
- show mld snooping interface

clear mld snooping

Use this command to clear MLD snooping groups and interface.

Command Syntax

```
clear mld snooping group *
clear mld snooping group X.X.X.X (IFNAME|)
clear mld snooping interface IFNAME
```

Parameters

`*`	Displays all groups
`IFNAME`	The name of the VLAN interface
`X:X::X:X`	Multicast group Address

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0 and updated in OcNOS version 6.2.0.

Examples

```
#clear mld snooping group *
```

mld snooping

Use this command to enable/disable MLD snooping on VLAN interfaces. When this command is given at the VLAN interface level, mld snooping can be enabled/disabled for that VLAN.

Use the `no` parameter with this command to globally disable MLD Snooping, or for the specified interface.

Command Syntax

```
mld snooping (enable|disable)
no mld snooping
```

Parameters

None

Default

By default, MLD Snooping is enabled in global config mode.

Command Mode

Configure mode and Interface mode for VLAN interface.

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#int vlan1.100
(config-if)#mld snooping enable
(config-if)#mld snooping disable

(config)#mld snooping
%% Already enabled by default
(config)#no mld snooping
```

mld snooping fast-leave

Use this command to enable MLD snooping fast-leave processing. MLD group-membership is removed, as soon as an MLD leave group message is received without sending out a group-specific query.

Use the `no` parameter with this command to disable fast-leave processing.

Command Syntax

```
mld snooping fast-leave
no mld snooping fast-leave
```

Parameters

None

Default

By default, MLD Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping fast-leave
(config-if)#exit
```

mld snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for MLD snooping in that VLAN.

Use the `no` parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax

```
mld snooping mrouter interface IFNAME
no mld snooping mrouter interface IFNAME
```

Parameters

`IFNAME`	Specify the name of the interface.

Default

N/A

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping mrouter interface eth1
(config-if)#exit
```

mld snooping querier

Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

The MLD snooping querier uses the 0.0.0.0 source IP address, because it masquerades as a proxy MLD querier for faster network convergence. It does not start or automatically cease the MLD querier operation if it detects a query message from a multicast router. It restarts as MLD snooping querier if no queries are seen within another querier interval.

Note: This command can only be configured on VLAN interfaces.

Use the `no` parameter with this command to disable MLD querier configuration.

Command Syntax

```
mld snooping querier
no mld snooping querier
```

Parameters

None

Default

By default, MLD snooping querier is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping querier
(config-if)#exit
```

mld snooping report-suppression

Use this command to enable report suppression for MLD version 1.

Use the `no` parameter to disable report suppression.

Note: MLD Snooping command can only be configured on VLAN interfaces. MLD snooping report suppression is not supported on x86 and Qumran devices.

Command Syntax

```
mld snooping report-suppression
```

```
no mld snooping report-suppression
```

Parameters

None

Default

By default, MLD snooping report suppression is enabled on x86.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface vlan1.100
(config-if)#mld snooping report-suppression
(config-if)#exit
```

show debugging mld snooping

Use this command to display debugging information for MLD.

Command Syntax

```
show debugging mld snooping
```

Parameters

None

Default

N/A

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#show debugging mld snooping
MLD Snooping Debugging status:
  MLD Snooping Decoder debugging is on
  MLD Snooping Encoder debugging is on
  MLD Snooping Events debugging is on
  MLD Snooping FSM debugging is on
  MLD Snooping Tree-Info-Base (TIB) debugging is on
```

show mld snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax

```
show mld snooping mrouter (IFNAME|)
```

Parameters

IFNAME	The name of the VLAN interface

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#show mld snooping mrouter vlan1.100
VLAN      Interface       IP-address                 Expires
100       eth3(dynamic)   fe80::a00:27ff:fe6f:5bc1   00:02:16

#show mld snooping mrouter
VLAN      Interface         IP-address                      Expires
400       eth4(static)      --                              --
100       eth1(dynamic)     fe80::a00:27ff:fe27:9856        00:02:19
200       eth2(dynamic)     fe80::a00:27ff:fe32:7951        00:02:45
300       eth3(dynamic)     fe80::a00:27ff:feff:f063        00:01:51
```

show mld snooping statistics

Use this command to display MLD snooping statistics data.

Command Syntax

```
show mld snooping statistics
show mld snooping statistics (interface IFNAME|)
show mld snooping statistics (count)
```

Parameters

IFNAME	The name of the VLAN interface
Count	Consolidated group statistics

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show mld snooping statistics
MLD Snooping statistics for vlan1.300
 Group Count            :  2
 MLDv1 reports received :  0
 MLDv2 reports received :  2
 MLDv1 leaves received  :  0
 MLDv1 query warnings   :  0
 MLDv2 query warnings   :  0

#show mld snooping statistics count
MLD Snooping consolidated statistics
Total number of groups              :  2
Total MLDv1 reports received        :  0
Total MLDv2 reports received        :  4
Total MLDv1 leaves received         :  2
Total MLDv1 query warnings          :  0
Total MLDv2 query warnings          :  0

#show mld snooping statistics interface vlan1.100
MLD Snooping statistics for vlan1.100
 Group Count                          :  0
 MLDv1 reports received               :  0
 MLDv2 reports received               :  2
 MLDv1 leaves received                :  1
 MLDv1 query warnings                 :  0
 MLDv2 query warnings                 :  0
```

show mld snooping groups

Use this command to display MLD snooping groups.

Command Syntax

```
show mld snooping groups
show mld snooping groups (IFNAME|)
show mld snooping groups (IFNAME|) detail
show mld snooping groups X.X.X.X
show mld snooping groups X.X.X.X detail.
```

Parameters

`IFNAME`	The name of the VLAN interface
`X:X::X:X`	Address of multicast group
`detail`	MLDv2 source information

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#sh mld snooping groups detail
MLD Connected Group Membership Details for eth3
Interface:      eth3
Group:          ff1e::10
Uptime:         00:00:10
Group mode:     Include ()
Last reporter:  fe80::a00:27ff:febb:5235
Group source list: (R - Remote, M - SSM Mapping, S - Static )
Source Address   Uptime             v2 Exp       Fwd    Flags
3000::10         00:00:10           00:04:09   Yes       R
```

show mld snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax

```
show mld snooping interface (IFNAME|)
```

Parameters

IFNAME	Name of the interface.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#sh mld snooping interface vlan1.100
 MLD Snooping information for vlan1.100 (Index 9)
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Active, Non-Querier,
 Internet address is fe80::a00:27ff:fe8d:e47a
 MLD querying router is :
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is not enabled
 MLD Snooping report suppression is disabled
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 0
 Active Ports:
  eth2
```

Multicast Command Reference

CHAPTER 1 Multicast Commands

OcNOS multicast protocol modules work with the Multicast Routing Information Base (MRIB).

- clear ip mroute
- debug ip mrib
- ip mroute
- ip multicast route-limit
- ip multicast ttl-threshold
- ip multicast-routing
- ip multicast bidirectional enable
- l2 unknown mcast
- ipv6 mroute
- show debugging ip mrib
- show ip mroute
- show ip mvif
- show ip multicast rpa
- show running-config interface multicast
- snmp restart mribd

© 2026 IP Infusion Inc. Proprietary

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
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) A.B.C.D <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.
`<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
```

ip multicast bidirectional enable

Data Plane may require specific resource allocations for enabling multipoint to multipoint (bidirectional) multicast data forwarding.

Use this command to configure data plane for such resource allocation.

Use the `no` form of this command to revert this configuration.

Dependent on feature VLAN classifier, multicast bidirectional and VLAN classifier are dependent on same hardware resource so they are made mutually exclusive. Disable VLAN classifier to enable this feature.

Command Syntax

```
ip multicast bidirectional enable
```

```
no ip multicast bidirectional enable
```

Parameters

None

Default

By default, bidirectional forwarding is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#ip multicast bidirectional enable
```

l2 unknown mcast

Use this command to either forward the unknown multicast traffic to all ports (except the ingress port) within the VLAN or to drop it.

Note: Before configuring this command, configure the L2 bridge first.

Command Syntax

```
l2 unknown mcast (flood|discard)
```

Parameters

discard	The switch does not forward multicast traffic for groups with no known members. Instead of flooding the multicast packets to all ports within the VLAN, the switch simply drops or discards the unknown multicast traffic.
flood	The switch forwards multicast traffic to all ports (except the ingress port) within the VLAN, treating it similar to broadcast traffic. This ensures that even if the switch is not aware of the multicast group memberships for certain ports, all devices within the VLAN receive the multicast packets.

.

Default

L2 unknown multicast traffic is set to flood.

Command Mode

Configuration mode

Applicability

Introduced in the OcNOS version 6.5.1.

Example

The following command forwards the multicast traffic to all ports.

```
OcNOS#configure terminal
(config)#l2 unknown mcast flood
```

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
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X <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.
`<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
```

The following is a sample output for this command displaying the IP multicast routing table for Bidirectional routes:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(*, 225.0.0.0)/24, uptime 00:01:53
Owner PIM, Flags: FB
RPA ID: 4
Outgoing interface list:
vlan1.10 (1)

(*, 225.0.0.1)/32, uptime 00:00:20
Owner PIM, Flags: FB
RPA ID: 4
Outgoing interface list:
vlan1.10 (1)
vlan1.20 (1)
```

Table 1-1: 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 1-2: Show ip mroute output

Entry	Description
(a.d.c.d, 224.x.x.x)	Source Address paired with its Destination Multicast Group Address
uptime	As stated.
Owner	The owner is derived from the multicast group notable address (IANA). In the example above, the owner is specified as PIM because it is using the IANA address: 224.0.0.13. Other owners can be OSPF (224.0.0.5), IS-IS (224.0.0.19–21), and so on.
Flags	The flags associated with this mroute table entry.
Incoming interface	The name of the in coming interface (eth1, xe5/2, etc.).
Outgoing interface list	A numbered list of the outgoing interfaces

Table 1-3: 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 1-4: 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 1-4: Show ip mvif output (Continued)

Entries	Description
TTL	Time to Live for the entry.
Local Address	AS stated.
Remote Address	As stated.
Uptime	How long the multicast interface has been operating.

show ip multicast rpa

Bidirectional (multipoint to multipoint) multicast forwarding uses a list of incoming interfaces. These interface list is created for each bidirectional RP. Such an entity is identified with an id number. When a bidirectional route object is programmed, this id would be used to indicate it'sits incoming interface list. This command outputs this entity list. Use this command to display the MRIB rpa details.

Command Syntax

show ip multicast rpa

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 4.0.

Example

```
#show ip multicast rpa

IP Multicast bidir rpa
2.2.2.2:1 uptime 00:23:16
  Incoming interface list:
      vlan1.50 (3)
      vlan1.30 (0)
      vlan1.40 (2)
```

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 IPv6 Multicast Commands

OcNOS multicast protocol modules work with the Multicast Routing Information Base (MRIB).

Note: Supported only in Qumran2 platforms.

- clear ipv6 mroute
- debug ipv6 mrib
- ipv6 mroute
- ipv6 multicast route-limit
- ipv6 multicast-routing
- ipv6 mroute
- show debugging ipv6 mrib
- show ipv6 mroute
- show ipv6 mif
- show running-config interface ipv6 multicast
- snmp restart mrib

© 2026 IP Infusion Inc. Proprietary

clear ipv6 mroute

Use this command to delete entries from the IPv6 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 ipv6 mroute *
clear ipv6 mroute X:X::X:X
clear ipv6 mroute X:X::X:X X:X::X:X
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 X:X::X:X pim sparse-mode
clear ipv6 mroute X:X::X:X X:X::X:X pim (dense mode| sparse-mode)
clear ipv6 mroute (vrf NAME|) *
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|) 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
clear ipv6 mroute (vrf Name|) X:X::X:X pim sparse-mode
clear ipv6 mroute (vrf Name|) X:X::X:X X:X::X:X pim (dense-mode | sparse-mode)
```

Parameters

`*`	All multicast routes.
`X:X::X:X`	Group IPv6 address.
`X:X::X:X`	Source IPv6 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 in OcNOS version 6.2.0.

Example

```
#clear ip mroute vrf VRF_A 1001::12 ff0e::1/128
```

debug ipv6 mrib

Use this command to set debug options for IPv6 multicast.

Use the `no` parameter with this command to disable debugging IPv6 multicast.

Command Syntax

```
debug ipv6 mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
debug ipv6 mrib (vrf NAME|)(all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ipv6 mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ipv6 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 in OcNOS version 6.2.0.

Example

```
#debug ipv6 mrib all
```

ipv6 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

```
ipv6 mroute (vrf NAME|) X:X::X:X (static|rip|ospf|bgp|isis|) X:X::X:X
ipv6 mroute (vrf NAME|) X:X::X:X (static|rip|ospf|bgp|isis|) X:X::X:X <1-255>
no ipv6 mroute (vrf NAME|) X:X::X:X (static|rip|ospf|bgp|isis|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`X:X::X:X`	Multicast source IPv6 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.
`X:X::X:X`	IPv6 address to use as the RPF address. A host IPv6 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.
`<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 in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#ipv6 mroute ff0e::1/128 1001::12

#configure terminal
(config)#ipv6 mroute vrf VRF_A ff0e::1/128 1001::12 1
```

ipv6 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

```
ipv6 multicast route-limit <1-2147483647>
ipv6 multicast route-limit <1-2147483647> <1-2147483647>
ipv6 multicast (vrf NAME|) route-limit <1-2147483647>
ipv6 multicast (vrf NAME|) route-limit <1-2147483647> <1-2147483647>
no ipv6 multicast route-limit
no ipv6 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)#ipv6 multicast route-limit 34 24
```

ipv6 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

```
ipv6 multicast-routing
ipv6 multicast-routing (vrf NAME|)
no ipv6 multicast-routing
no ipv6 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 in OcNOS version 6.2.0.

Example

```
#configure terminal
(config)#ipv6 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
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X <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.
`<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 in OcNOS version 6.2.0.

Example

```
(config)#ipv6 mroute 10:10::10:10/64 10:10::10:12 1
```

show debugging ipv6 mrib

Use this command to display IPv6 multicast debugging information.

Command Syntax

```
show debugging ipv6 mrib
show debugging ipv6 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 in OcNOS version 6.2.0.

Examples

The following is a sample output of the `show debugging ipv6 mrib` command.

```
#show debugging ipv6 mrib
MRIBv6 debugging status:
  MRIBv6 event debugging is on
  MRIBv6 route debugging is on
```

show ipv6 mroute

Use this command to display the IPv6 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 ipv6 mroute (dense|sparse|) (count|summary|)
show ipv6 mroute X:X::X:X (dense|sparse|)(count|summary|)
show ipv6 mroute X:X::X:X X:X::X:X (dense|sparse|) (count|summary|)
show ipv6 mroute (vrf NAME|) (dense|sparse|) (count|summary|)
show ipv6 mroute (vrf NAME|) X:X::X:X (dense|sparse|) (count|summary|)
show ipv6 mroute (vrf NAME|) X:X::X:X X:X::X:X (dense|sparse|) (count|summary|)
```

Parameters

`X:X::X:X`	Source or Group IPv6 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 in OcNOS version 6.2.0.

Example

The following is a sample output of this command displaying the IPv6 multicast routing table, with and without specifying the group and source IPv6 address:

```
rtr6#show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface

(5001::2, ff3e::1), uptime 00:00:16, stat expires 00:03:14
Owner PIM, Flags: TF
  Incoming interface: xe17
  Outgoing interface list:
    xe18 (1)
```

show ipv6 mif

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 ipv6 mif
show ipv6 mif IFNAME
show ipv6 mif (vrf NAME|)
show ipv6 mif (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 in OcNOS version 6.2.0.

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 ipv6 mif
Interface Mif   Owner                    TTL  Uptime
          Idx   Module
ce9       0     PIM                      1    00:00:04
Register  1     PIM                      1    00:00:04
ce10      2     PIM                      1    00:00:04
```

show running-config interface ipv6 multicast

Use this command to show the running system status and configuration for an IPv6 multicast interface.

Command Syntax

```
show running-config interface IFNAME ipv6 multicast
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

```
#show running-config interface ce9 ipv6 multicast
!
interface ce9
!
```

snmp restart mrib

Use this command to restart SNMP in Multicast Routing Information Base (MRIB)

Command Syntax

```
snmp restart mrib
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#snmp restart mrib
```

CHAPTER 3 Layer 3 MLD Multicast Commands

This chapter describes the commands for Multicast Listener Discovery (MLD) which includes the MLD proxy service.

Note: Supported only in Qumran2 platforms.

- clear ipv6 mld
- debug ipv6 mld
- ipv6 mld
- ipv6 mld access-group
- ipv6 mld immediate-leave
- ipv6 mld last-member-query-count
- ipv6 mld last-member-query-interval
- ipv6 mld limit
- ipv6 mld mroute-proxy
- ipv6 mld proxy unsolicited-report-interval
- ipv6 mld proxy-service
- ipv6 mld querier-timeout
- ipv6 mld query-interval
- ipv6 mld query-max-response-time
- ipv6 mld robustness-variable
- ipv6 mld ssm-map enable
- ipv6 mld ssm-map static
- ipv6 mld startup-query-count
- ipv6 mld startup-query-interval
- ipv6 mld static-group
- ipv6 mld version
- show debugging ipv6 mld
- show ipv6 mld groups
- show ipv6 mld interface
- show ipv6 mld proxy
- show ipv6 mld ssm-map

© 2026 IP Infusion Inc. Proprietary

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 in OcNOS version 6.2.0.

Example

```
#clear ipv6 mld group *
#clear ipv6 mld group 1001::12
#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 in OcNOS version 6.2.0.

Example

```
#configure terminal
(config)#debug ipv6 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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 unsolicited-report-interval

Use this command to set an unsolicited report interval for an interface designated as an MLD proxy (upstream hostside).

Use the `no` parameter with this command to remove the unsolicited report interval from the interface.

Command Syntax

```
ipv6 mld proxy unsolicited-report-interval <1000-25500>
no ipv6 mld 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 in OcNOS version 6.2.0

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 mld proxy unsolicited-report-interval 1234
(config-if)#no ipv6 mld proxy unsolicited-report-interval
```

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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

Configure mode

Applicability

This command was introduced in OcNOS version 6.2.0.

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

Configure mode

Applicability

This command was introduced in OcNOS version 6.2.0.

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 startup-query-count

Use this command to set a startup query count for MLD.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ipv6 mld startup-query-count <2-10>
no ipv6 mld 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 in OcNOS version 6.2.0.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld startup-query-count 2

(config-if)#no ipv6 mld startup-query-count
```

ipv6 mld startup-query-interval

Use this command to set a query interval value for MLD.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ipv6 mld startup-query-interval <1-18000>
no ipv6 mld 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 in OcNOS version 6.2.0.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld startup-query-interval 1

(config-if)#no ipv6 mld startup-query-interval
```

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

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 in OcNOS version 6.2.0.

Example

The following command displays local-membership information for all interfaces:

```
#show ipv6 mld groupsOcNOS version 6.1.0
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 3-1: 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 3-1: 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 reporter 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 in OcNOS version 6.2.0.

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 3-2: 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 3-2: 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 proxy

Use this command to display the state of MLD Proxy services for a specified interface or for all interfaces.

Command Syntax

```
show ipv6 mld proxy groups (detail|)
show ipv6 mld proxy groups X:X::X:X (detail|)
show ipv6 mld proxy groups IFNAME (detail|)
show ipv6 mld proxy groups IFNAME X:X::X:X (detail|)
show ipv6 mld (vrf NAME|) proxy groups (detail|)
show ipv6 mld (vrf NAME|) proxy groups X:X::X:X (detail|)
show ipv6 mld (vrf NAME|) proxy groups IFNAME (detail|)
show ipv6 mld (vrf NAME|) proxy groups IFNAME X:X::X:X (detail|)
```

Parameters

`vrf`	Specify the VRF name.
`groups`	MLD proxy group membership information.
`X:X::X:X`	Address of multicast group.
`IFNAME`	The name of the VLAN interface.
`detail`	MLDv3 source information

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

```
#show ipv6 mld proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1

#show ipv6 mld proxy groups

MLD Connected Proxy Group Membership
Group Address  Interface   State   Member state
1001::12       eth1        Active  Delay
```

Table 3-31 explains the output fields.

Table 3-3: show ipv6 mld 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 3-32 explains the output fields.

Table 3-4: show ipv6 mld 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 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 in OcNOS version 6.2.0.

Example

The following is an example of this command:

```
#show ipv6 mld ssm-map
SSM Mapping : Enabled
Database    : None configured
```

Index

A

accept-lifetime 353

B

begin modifier 20
BGP community value
  command syntax 19
Bootstrap Router 99
bootstrap router 261, 315
braces
  command syntax 18
BSR 99, 261, 315
BSR validation 114

C

candidate status 307
clear ip igmp 48
clear ip mroute 188, 269, 365, 384
clear ip msdp sa-cache 191
clear ip pim sparse-mode bsr 192
clear ip pim sparse-mode bsrt 271
clear ipv6 mld 396
command abbreviations 16
command completion 16
command line
  errors 17
  help 15
  keyboard operations 19
command modes 23
  configure 23
  exec 23
  interface 23
  privileged exec 23
  router 23
command negation 17
command syntax
  ? 18
  . 18
  () 17, 18
  {} 18
  | 17
  A.B.C.D/M 18
  AA:NN 19
  BGP community value 19
  braces 18
  conventions 17
  curly brackets 18
  HH:MM:SS 18
  IFNAME 18
  interface name 18
  IPv4 address 18
  IPv6 address 18
  LINE 18
  lowercase 17
  MAC address 19
  monospaced font 17
  numeric range 19
  parantheses 18
  parentheses 17
  period 18
  question mark 18
  square brackets 18
  time 18
  uppercase 17
  variable placeholders 18
  vertical bars 17
  WORD 18
  X:X::X:X 18
  X:X::X:X/M 18
  XX:XX:XX:XX:XX:XX 19
configure
  IGMP snooping 43
configure mode 23
configuring BSR
  BSR topology 113
  validation commands 114
configuring RP dynamically 109
configuring RP statically 103, 163
curly brackets
  command syntax 18

D

data flow
  PIM-SM 99
debug igmp 49, 82
debug ip pim timer joinprune 200, 202
debug mld 397
debug pim packet 194, 273
debug pim sm sparse-mode timer assert 274
debug pim sparse-mode timer hello 276
debug pim sparse-mode timer register 202, 279
designated router priority 222, 290
downstream 99, 130

E

exec command mode 23

G

group-to-RP mappings 112

I

IFNAME 18
IGMP Commands
  clear ip igmp 48
  debug igmp 49, 82
  ip igmp 51
  ip igmp access-group 52

ip igmp immediate-leave 53
ip igmp last-member-query-count 55
ip igmp last-member-query-interval 56
ip igmp limit 57
ip igmp mroute-proxy 58
ip igmp proxy-service 60
ip igmp querier-timeout 62
ip igmp query-interval 63
ip igmp query-max-response-time 64
ip igmp robustness-variable 66
ip igmp snooping 84
ip igmp snooping fast-leave 85
ip igmp snooping mrouter 86
ip igmp snooping querier 87
ip igmp snooping report-suppression 88
ip igmp ssm-map enable 67
ip igmp ssm-map static 68
ip igmp static-group 69
ip igmp version 72
show ip igmp groups 74
show ip igmp interface 76
show ip igmp snooping mrouter 90
show ip igmp snooping statistics 96
IGMP snooping
configuration 43
interface mode 23
ip igmp 51
ip igmp access-group 52
ip igmp immediate-leave 53
ip igmp last-member-query-count 55
ip igmp last-member-query-interval 56
ip igmp limit 57
ip igmp mroute-proxy 58
ip igmp proxy-service 60
ip igmp querier-timeout 62
ip igmp query-interval 63
ip igmp query-max-response-time 64
ip igmp robustness-variable 66
ip igmp snooping 84
ip igmp snooping fast-leave 85
ip igmp snooping mrouter 86
ip igmp snooping querier 87
ip igmp snooping report-suppression 88
ip igmp ssm-map enable 67
ip igmp ssm-map static 68
ip igmp static-group 69
ip igmp version 72
ip mroute 367, 386
ip msdp default-peer 203
ip msdp mesh-group 204
ip msdp originator-id 205
ip msdp password 206
ip msdp peer 207
ip multicast route-limit command 368, 387
ip multicast ttl-threshold 369, 388
ip multicast-routing 370, 388
ip pim accept-register list 208, 280
ip pim anycast-rp 211, 282
ip pim bsr-border 217, 286
ip pim bsr-candidate 220, 287
ip pim cisco-register-checksum 221, 288
ip pim dr-priority 222, 290
ip pim exclude-genid 224, 292
ip pim hello-holdtime 225, 293
ip pim hello-interval 226, 294
ip pim ignore-rp-set-priority 227, 295
ip pim jp-timer 228, 296
ip pim neighbor-filter 229, 297
ip pim register-candidate 240, 307
ip pim register-candidate group-list 307
ip pim register-rate limit 232, 300
ip pim register-rp-reachability 234, 301
ip pim register-source 235, 302
ip pim rp-address 238, 305
ip pim rp-register-kat 308
ip pim spt-threshold 242, 310
ip pim ssm 243, 311
ip pim unicast-bsm 245, 313
IPv4 address
command syntax 18
IPv6 address
command syntax 18
ipv6 mld 399
ipv6 mld access-group 400
ipv6 mld immediate-leave 401
ipv6 mld last-member-query-count 402
ipv6 mld last-member-query-interval 403
ipv6 mld limit 404
ipv6 mld mroute-proxy 405
ipv6 mld proxy-service 407
ipv6 mld querier-timeout 408
ipv6 mld query-interval 409
ipv6 mld query-max-response-time 410
ipv6 mld robustness-variable 411
ipv6 mld ssm-map enable 412
ipv6 mld ssm-map static 413
ipv6 mld static-group 416
ipv6 mld version 417
ipv6 mroute 373, 389
IS-IS commands
accept-lifetime 353

L

LINE 18

M

MAC address
command syntax 19
MLD Commands
clear ipv6 mld 396
debug mld 397
ipv6 mld 399
ipv6 mld access-group 400
ipv6 mld immediate-leave 401
ipv6 mld last-member-query-count 402
ipv6 mld last-member-query-interval 403

ipv6 mld limit 404
ipv6 mld mroute-proxy 405
ipv6 mld proxy-service 407
ipv6 mld querier-timeout 408
ipv6 mld query-interval 409
ipv6 mld query-max-response-time 410
ipv6 mld robustness-variable 411
ipv6 mld ssm-map enable 412
ipv6 mld ssm-map static 413
ipv6 mld static-group 416
ipv6 mld version 417
show ipv6 mld groups 419
show ipv6 mld interface 421
MRIB 98
MSDP 169
Multicast Commands
clear ip mroute 365, 384
debug ip mrib
debug ip mrib 366, 385
ip mroute 367, 386
ip multicast route-limit 368, 387
ip multicast ttl-threshold 369, 388
ip multicast-routing 370, 388
show ip mroute 375, 391
show ip mvif 378, 392
multicast routing 370, 388
multicast routing table, displaying 255, 320
multicast routing table, displaying based on address 320

P

parantheses
command syntax 18
parentheses
command syntax 17
period
command syntax 18
PIM-DM configuration 37, 175, 338
downstream 130
terminology 130
PIM-SM commands
clear ip mroute 188, 269
clear ip msdp sa-cache 191
clear ip pim sparse-mode bsr 192, 271
debug ip pim timer joinprune 200, 202
debug pim packet 194, 273
debug pim sparse-mode timer assert 274
debug pim sparse-mode timer hello 276
debug pim sparse-mode timer register 202, 279
ip msdp default-peer 203
ip msdp mesh-group 204
ip msdp originator-id 205
ip msdp password 206
ip msdp peer 207
ip pim accept-register list 208, 280
ip pim anycast-rp 211, 282
ip pim bsr-border 217, 286
ip pim bsr-candidate 220, 287
ip pim cisco-register-checksum 221, 288
ip pim dr-priority 222, 290
ip pim exclude-genid 224, 292
ip pim hello-holdtime 225, 293
ip pim hello-interval 226, 294
ip pim ignore-rp-set-priority 227, 295
ip pim jp-timer 228, 296
ip pim neighbor-filter 229, 297
ip pim register-rate limit 232, 300
ip pim register-rp-reachability 234, 301
ip pim register-source 235, 302
ip pim rp-address 238, 305
ip pim rp-candidate 240, 307
ip pim rp-candidate group-list 307
ip pim rp-register-kat 308
ip pim ssm 243, 311
ip pim unicast-bsm 245, 313
show debugging pim 246, 314
show ip msdp sa-cache 249
show ip pim bsr-router 252
show ip pim rp mapping 328
show ip pim rp-hash 264, 327
PIM-SM configuration 98
bootstrap router 99
configuring RP dynamically 109
configuring RP statically 103, 163
data flow from source to receivers 99
determining the RP 99
downstream 99
electing a designated router 99
forwarding multicast packets 100
group-to-RP mappings 112
joining the shared tree 100
Multicast Routing Information Base 98
pruning the interface 100
references 98, 163
registering with the RP 100
rendezvous point 98
reverse path forwarding 98, 130
sending out Hello messages 99
sending Register-Stop messages 100
shared trees 99
source-based trees 99
terminology 163
tree information base 98
upstream 98
PIMv4 Commands 186
Privileged Exec mode
show ip pim rp mapping 328
privileged exec mode 23

Q

question mark
command syntax 18

R

references
PIM-SM 98, 163

Rendezvous Point 98
rendezvous point
  candidate status 307
  mappings 265
Reverse Path Forwarding 98, 130
root of the tree 98
router mode 23
RP 98
RPF 98, 130, 169

S

shared trees 99
show commands 20
  exclude modifier 22
  include modifier 21
  redirect modifier 22
show debugging pim 246, 314
show ip igmp groups 74
show ip igmp interface 76
show ip igmp snooping mrouter 90
show ip igmp snooping statistics 96
show ip mroute 375, 391
show ip msdp sa-cache 249
show ip mvif 378, 392
show ip pim bsr-router 252
show ip pim rp mapping 328
show ip pim rp-hash 264, 327
show ipv6 mld groups 419
show ipv6 mld interface 421
show running-config interface igmp 81
show running-config interface multicast 381, 393
source-based trees 99
square brackets
  command syntax 18

T

terminology
  PIM-DM 130
  PIM-SM 163
TIB 98
time
  command syntax 18
Tree Information Base 98

V

vertical bars
  command syntax 17

W

WORD 18